

Internet of Things

Uttam Ghosh  
Chinmay Chakraborty  
Lalit Garg  
Gautam Srivastava *Editors*

# Intelligent Internet of Things for Healthcare and Industry



Springer

# **Internet of Things**

Technology, Communications and Computing

## **Series Editors**

Giancarlo Fortino, Rende (CS), Italy

Antonio Liotta, Edinburgh Napier University, School of Computing,  
Edinburgh, UK

The series Internet of Things - Technologies, Communications and Computing publishes new developments and advances in the various areas of the different facets of the Internet of Things. The intent is to cover technology (smart devices, wireless sensors, systems), communications (networks and protocols) and computing (theory, middleware and applications) of the Internet of Things, as embedded in the fields of engineering, computer science, life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in the Internet of Things research and development area, spanning the areas of wireless sensor networks, autonomic networking, network protocol, agent-based computing, artificial intelligence, self organizing systems, multi-sensor data fusion, smart objects, and hybrid intelligent systems.

\*\* Indexing: *Internet of Things* is covered by Scopus and Ei-Compendex \*\*

More information about this series at <https://link.springer.com/bookseries/11636>

Uttam Ghosh • Chinmay Chakraborty • Lalit Garg  
Gautam Srivastava  
Editors

# Intelligent Internet of Things for Healthcare and Industry

 Springer



*Editors*

Uttam Ghosh   
Vanderbilt University  
Nashville, TN, USA

Chinmay Chakraborty   
Electronics & Communication Engineering  
Birla Institute of Technology  
Jharkhand, India

Lalit Garg  
Information and Communication  
Technology  
University of Malta  
Msida, Malta

Gautam Srivastava   
Mathematics and Computer Science  
Brandon University  
Brandon, MB, Canada

ISSN 2199-1073

ISSN 2199-1081 (electronic)

Internet of Things

ISBN 978-3-030-81472-4

ISBN 978-3-030-81473-1 (eBook)

<https://doi.org/10.1007/978-3-030-81473-1>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*To my family. Uttam Ghosh*

*To Arjun and Krishna. Gautam Srivastava*

# Preface

## Motivations for This Book

The Internet of Things (IoT) is made up of software components and physical objects that are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple behavioral modalities and interacting with each other and with the users. They can interact directly with data and access services using a myriad of ways that change with their context of use. Smart grids, global environmental and disaster monitoring systems, medical and homeland security systems as well as autonomous transportation, and automatic pilot avionics are the main applications of IoT.

Data analytics has a significant role to play in the growth and success of IoT applications toward expert processing of huge process-level data. The utilization of data analytics shall, therefore, be promoted in the area of IoT to gain improved revenues, competitive gain, and customer engagement. In recent years, machine learning approaches have emerged as powerful computational models and have shown significant success to deal with a massive amount of data in unsupervised settings. The emerging technologies of cyber-physical systems, wearable devices, cloud computing, and data analytics offer the potential of acquiring and processing a tremendous amount of data from the physical world. Promising computing paradigms and advanced technologies (e.g., smart home or city) relating to context awareness systems, activity recognition, distributed smart sensing, heterogeneous big data analytics, and machine learning have been increasingly developed and integrated into IoT to make it a reality. Learning analytics provides new impulses for the development and application of cyber-physical systems.

*Intelligent Internet of Things for Healthcare and Industry* focuses on emerging trends, strategies, and applications of IoT in both healthcare and industry from a data analytics perspective. IoT systems will continuously generate massive data that requires big data techniques to process and help to improve system security, efficiency, and scalability. Data analytics are relevant for healthcare as well as industry to meet many technical challenges and issues that need to be addressed

to realize this potential. The advanced healthcare systems have to be upgraded with new capabilities such as data analytics, machine learning, intelligent decision-making, and more professional services. IoT helps to design and develop intelligent medical and industry solutions assisted by data analytics and machine learning.

## Contents of This Book

*Intelligent Internet of Things for Healthcare and Industry* is made up of several state-of-the-art chapters from both scientists and practitioners working in IoT, healthcare, and AI. It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this area or those interested in grasping its diverse facets and exploring the latest advances in the field. More specifically, the book contains 17 chapters, split into two main parts. Part I focuses on IoT in healthcare, while Part II is about the Intelligent IoT in the industry. Chapter 1 examines the effectiveness of machine and deep learning on IoT healthcare devices. Chapter 2 features an in-depth look into network protocols on the Internet of Health Things (IoHT). Chapter 3 examines affective computing in e-health using remote IoT. Chapter 4 investigates the COVID-19 pandemic and ways IoT can help fight its ramifications. Chapter 5 looks at patient health monitoring using IoT sensors. In Chap. 6, blockchain is implemented for secure smart healthcare systems. Chapter 7 examines the impact of computation intelligence on the healthcare systems emphasizing bioinformatics and the Internet of Medical Things. A very in-depth survey of security and privacy in the Internet of Medical Things is given in Chap. 8. Chapter 9 presents an exploration into wearable sensor technology in healthcare. In Chap. 10, diabetes prediction is examined using a fog-based infrastructure. A comprehensive analysis of IoT sustainability in a post-COVID era is given in Chap. 11. Diagnosis of autism is investigated in Chap. 12 using optimization algorithms. Moving away from healthcare in the second part of the book, Chap. 13 dives into machine learning and fog computing areas for smart cities. In Chap. 14, quality of service and green computing is investigated for industry. Chapter 15 looks at privacy issues for smart IoT networks in industry. In Chap. 16, Industry 4.0 is surveyed in the automotive field. To conclude, Chap. 17 implements smart security for industrial applications.

## Acknowledgments

We want to take this opportunity and express our thanks to the contributors to this volume and the reviewers for their great efforts in reviewing and providing interesting feedback to the authors of the chapters. The editors would like to thank Dr. Giancarlo Fortino (Springer, Series Editor), Dr. Antonio Liotta (Springer, Series Editor), and Ms. Cynthia Pushparaj (Springer Project Coordinator) for the

editorial assistance and support to produce this important scientific work. Without this collective effort, this book could not have been completed.

Overall, *Intelligent Internet of Things for Healthcare and Industry* aims at promoting and facilitating exchanges of research knowledge and findings across different disciplines.

Brandon, MB, Canada

Gautam Srivastava

Msida, Malta

Lalit Garg

Jharkhand, India

Chinmay Chakraborty

Nashville, TN, USA

Uttam Ghosh

# Contents

<b>Effectiveness of Machine and Deep Learning in IOT-Enabled Devices for Healthcare System</b> .....	1
Yogesh Kumar and Ruchi Singla	
<b>Network Protocols for the Internet of Health Things</b> .....	21
Trisha Das Mou and Gautam Srivastava	
<b>Affective Computing for eHealth Using Low-Cost Remote Internet of Things-Based EMG Platform</b> .....	67
Žygintas Tamulis, Mindaugas Vasiljevas, Robertas Damaševičius, Rytis Maskeliunas, and Sanjay Misra	
<b>Application of the Internet of Things (IoT) to Fight the COVID-19 Pandemic</b> .....	83
Roseline Oluwaseun Ogundokun, Joseph Bamidele Awotunde, Emmanuel Abidemi Adeniyi, and Sanjay Misra	
<b>An Enhanced IoT-Based Array of Sensors for Monitoring Patients' Health</b> .....	105
Modupe Odusami, Sanjay Misra, Olusola Abayomi-Alli, Shobayo Olamilekan, and Chukwuebuka Moses	
<b>A Secured Smart Healthcare Monitoring Systems Using Blockchain Technology</b> .....	127
Joseph Bamidele Awotunde, Chinmay Chakraborty, and Sakinat Oluwabukonla Folorunso	
<b>Computational Intelligence in Healthcare with Special Emphasis on Bioinformatics and Internet of Medical Things</b> .....	145
Siddharth Banyal, Deepanjali Mehra, Amartya, Siddhant Banyal, Deepak Kumar Sharma, and Uttam Ghosh	

**A Review on Security and Privacy of Internet of Medical Things** ..... 171  
Mohan Krishna Kagita, Navod Thilakarathne, Thippa Reddy Gadekallu,  
and Praveen Kumar Reddy Maddikunta

**An Introduction to Wearable Sensor Technology** ..... 189  
Arthur Medeiros, Lucas Leme, and Gautam Srivastava

**A Fog-Based Intelligent Secured IoMT Framework for Early  
Diabetes Prediction** ..... 199  
Dukka Karun Kumar Reddy, H. S. Behera, Janmenjoy Nayak,  
Ashanta Ranjan Routray, Pemmada Suresh Kumar, and Uttam Ghosh

**A Comprehensive Analysis of Sustainable IoT Infrastructure in  
the Post-COVID-19 Era** ..... 219  
Deepsubhra Guha Roy

**Reinforced Rider Optimization Algorithm for Diagnosis  
of Autism Spectrum Disorder and Medical Data** ..... 239  
N. B. Arunekumar and K. Suresh Joseph

**Machine Learning for Fog Computing-Based IoT Networks in  
Smart City Environment** ..... 267  
Subhendu Ghosh, Vinod Chandra, and Aneek Adhya

**QoS and Energy Efficiency Using Green Cloud Computing** ..... 287  
Riman Mandal, Sourav Banerjee, Md Bagbul Islam, Pushpita Chatterjee,  
and Utpal Biswas

**Privacy Issues in Smart IoT for Healthcare and Industry** ..... 307  
Kateryna Mokliakova and Gautam Srivastava

**Intelligent IoT for Automotive Industry 4.0: Challenges,  
Opportunities, and Future Trends** ..... 327  
Raj Krishan Ghosh, Anindya Banerjee, Prasenjit Aich, Deborsi Basu,  
and Uttam Ghosh

**Smart Security for Industrial and Healthcare IoT Applications** ..... 353  
M. Aruna, S. Ananda Kumar, B. Arthi, and Uttam Ghosh

**Index** ..... 373

# About the Editors

**Uttam Ghosh** joined Meharry Medical College as Associate Professor of Cybersecurity in the School of Applied Computational Sciences in January 2022. Earlier, he worked as an assistant professor of the practice in the Department of Computer Science at Vanderbilt University, where he was awarded the 2018–2019 Junior Faculty Teaching Fellow (JFTF).

Dr. Ghosh obtained his Master of Science and doctorate in electronics and electrical communication engineering from the Indian Institute of Technology (IIT) Kharagpur, India, in 2009 and 2013, respectively. He has postdoctoral experiences at the University of Illinois in Urbana-Champaign, Fordham University, and Tennessee State University. Dr. Ghosh has published more than 80 papers in reputed international journals by IEEE Transactions, Elsevier, Springer, IET, Wiley, InderScience, and IETE, and also in top international conferences sponsored by IEEE, ACM, and Springer. He has coedited and published three books: *Internet of Things and Secure Smart Environments*, *Machine Intelligence and Data Analytics for Sustainable Future Smart Cities*, and *Efficient Data Handling for Massive Internet of Medical Things*. Dr. Ghosh has conducted several sessions and workshops related to cyber-physical systems (CPS), SDN, IoT, and smart cities as co-chair at top international conferences including IEEE GLOBECOM 2020-2021, IEEE MASS 2020, SECON 2019-20, CPSCOM 2019, and ICDCS 2017. He has also served as a technical program committee (TPC) member at renowned international conferences. Dr. Ghosh is associate editor of *Human-centric Computing and Information Sciences* and *International Journal of Computers and Applications*. He is also a reviewer for international journals by IEEE Transactions, Elsevier, Springer, and Wiley. He serves as a guest editor for special issues with *IEEE Sensors*, *IEEE Transaction on Industrial Informatics (TII)*, *IEEE Journal of Health Informatics (JBHI)*, *IEEE Transaction on Network Science and Engineering (TNSE)*, *ACM Transactions on Internet Technology (TOIT)*, *Elsevier Computers & Electrical Engineering*, *Computer Communications*, *Springer Cluster Computing, Multimedia Tools and Applications (MTAP)*, *Wiley Internet Technology Letters (ITL)*, *MDPI Sensors*, and *Future Internet*. Dr. Ghosh is co-editing five books on Smart IoT, security, and data



analysis with CRC Press and Springer. He is a senior member of the IEEE and a member of ACM and Sigma-Xi.

**Gautam Srivastava** (Senior Member, IEEE) has extensive guest editorial experience including IEEE Trans on Fuzzy Systems, IEEE Trans on Industrial Informatics, Computer Standards and Interfaces, Applied Stochastic Modeling and Business, and many others. Dr. Gautam Srivastava was awarded a B.Sc. from Briar Cliff University in Sioux City, Iowa, USA, in 2004, followed by an M.Sc. and Ph.D. from the University of Victoria in Victoria, British Columbia, Canada, in the years 2006 and 2012, respectively. He then worked for 3 years at the University of Victoria in the Department of Computer Science (Faculty of Engineering), where he was regarded as one of the top undergraduate professors in Computer Science Course Instruction at the university. From there in 2014 he started a tenure-track position at Brandon University in Brandon, Manitoba, Canada, where he currently is an assistant professor. Dr. G (as he is popularly known) is active in research in the fields of Data Mining and Big Data. During his 6-year academic career, he has published a total of 160 papers in high-impact conferences and journals. He has also given guest lectures at many Taiwan universities on Big Data. He currently has active research projects with other academics in Taiwan, Singapore, Canada, and the USA.

**Lalit Garg** is a senior lecturer in Computer Information Systems at the University of Malta, Malta, and an honorary lecturer at the University of Liverpool, UK. He has also worked as a researcher at the Nanyang Technological University, Singapore, and Ulster University, UK. His supervision experience includes more than 200 Master's dissertations and four PhD theses. He has published more than a hundred high-impact publications in refereed journals, conferences, and books and edited five books. Some of his articles awarded best paper awards. He has many patents in his name. He has delivered several keynote speeches and organized/chaired/co-chaired international conferences. He has also consulted numerous public and private organizations for their information system implementations. His research interests are missing data handling, machine learning, data mining, cloud computing, Internet of Things (IoT), mathematical and stochastic modeling, operational research, and their applications, especially in the healthcare domain. He participates in many EU and local funded projects, including a one million euros Erasmus+ Programme Capacity-Building project in the field of Higher Education (CBHE) titled Training for Medical education via innovative eTechnology (MediTec). The University of Malta has awarded him the 2021–2022 Research Excellence Fund of 60,000 EUR for exploring Novel Intelligent Computing Methods for healthcare requirements forecasting, allocation, and management (NICE-Healthcare). He was awarded a research studentship in healthcare modeling to carry out his PhD research studies in the Faculty of Computing and Engineering at Ulster University, UK. His doctoral research was nominated for the Operational Research Society Doctoral Prize “Most Distinguished Body of Research leading to the Award of a Doctorate in the field of OR.”

**Chinmay Chakraborty** is working as an assistant professor (Sr.) in the Department of Electronics and Communication Engineering, Birla Institute of Technology, Mesra, India. He worked at the Faculty of Science and Technology, ICFAI University, Agartala, Tripura, India, as a senior lecturer. He worked as a research consultant in the Coal India project at Industrial Engineering and Management, IIT Kharagpur. He worked as a project coordinator of the Telecommunication Convergence Switch project under the Indo-US joint initiative. He also worked as a Network Engineer in System Administration at MISPL, India. His main research interests include the Internet of Medical Things, Wireless Body Area Network, Wireless Networks, Telemedicine, m-Health/e-health, and Medical Imaging. Dr. Chakraborty has published 70 papers at reputed international journals, conferences, book chapters, and books. He is an editorial board member in the different journals and conferences. He is serving as a guest editor of MDPI—*Future Internet Journal*, Wiley—*Internet Technology Letters*, Springer—*Annals of Telecommunications*, and Springer—*International Journal of System Assurance Engineering and Management*; lead guest editor of IGI—*International Journal of E-Health and Medical Communications*, Springer—*Multimedia Tools and Applications*, TechScience CMC, Springer—*Interdisciplinary Sciences: Computational Life Sciences*, Inderscience—*International Journal of Nanotechnology*, BenthamScience—*Current Medical Imaging*, *Journal of Medical Imaging and Health Informatics*; lead series editor of CRC—*Advances in Smart Healthcare Technologies*; and associate editor of *International Journal of End-User Computing and Development*, and has conducted a session of SoCTA-19, ICICC-2019, Springer CIS 2020, SoCTA-20, and SoCPaR 2020, and he is also a reviewer for international journals including IEEE Access, IEEE Sensors, IEEE Internet of Things, Elsevier, Springer, Taylor & Francis, IGI, IET, TELKOMNIKA Telecommunication Computing Electronics and Control, and Wiley. Dr. Chakraborty is co-editing eight books on Smart IoMT, Healthcare Technology, and Sensor Data Analytics with CRC Press, IET, Pan Stanford, and Springer. He has served as a publicity chair member at renowned international conferences including IEEE Healthcom, IEEE SP-DLT. Dr. Chakraborty is a member of Internet Society, Machine Intelligence Research Labs, and Institute for Engineering Research and Publication. He received a Best Session Runner-up Award, Young Research Excellence Award, Global Peer Review Award, Young Faculty Award, and Outstanding Researcher Award. He was the speaker for AICTE, DST-sponsored FDP, and CEP Short Term Course.

# Effectiveness of Machine and Deep Learning in IOT-Enabled Devices for Healthcare System



Yogesh Kumar and Ruchi Singla

## 1 Introduction

In the modern era of the twenty-first century, IoT has become an integral part of our everyday lives. It is a framework that uses technology like sensors, network communication, artificial intelligence, and big data to provide real-life solutions, and these solutions and systems are designed for optimal control and performance. From smart grids and connected cars to the industrial Internet of Things, IoT has a wide range of applications in healthcare. An IoT model comprises of an end node device that can communicate with a back-end data source via a communication medium [1]. Data and control messages can be seamlessly exchanged across the IoT endpoint and a data center server. Other than this, IoT has also suffered certain shortcomings, such as platform fragmentation; lack of interoperability; security issues; privacy threats; difficulty of cleaning, processing, and interpreting the data gathered by the sensors; safety issues; complex design; a few ambiguous terminologies, etc. [2].

“Today, it has become industry-agnostic jargon to describe how technology is currently being embedded in multiple markets, including healthcare, and provides the way in which business is conducted. IoT is a boon to the healthcare sector as healthcare services are costlier, a number of chronic diseases are on the rise, basic healthcare amenities do not reach the majority of people, and a large section of society is unproductive, making people more prone to chronic diseases. It is also a bitter fact that technology can’t stop the population from ageing or eradicate chronic

---

Y. Kumar (✉)

Department of Computer Engineering, Indus Institute of Technology & Engineering, Indus University, Ahmedabad, Gujarat, India

R. Singla

Department of Research, Innovations, Sponsored Projects & Entrepreneurship, Chandigarh Group of Colleges, Mohali, Punjab, India

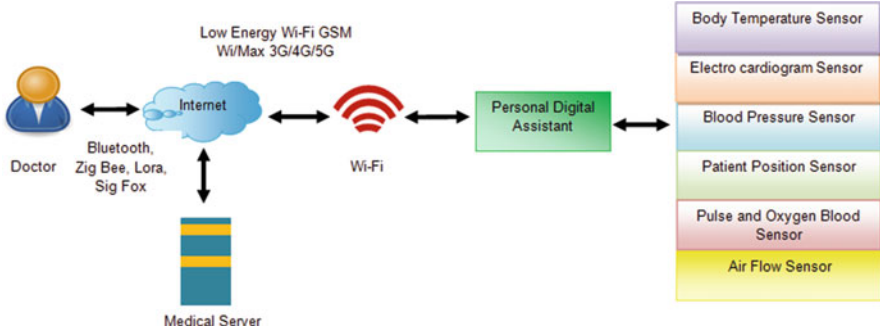


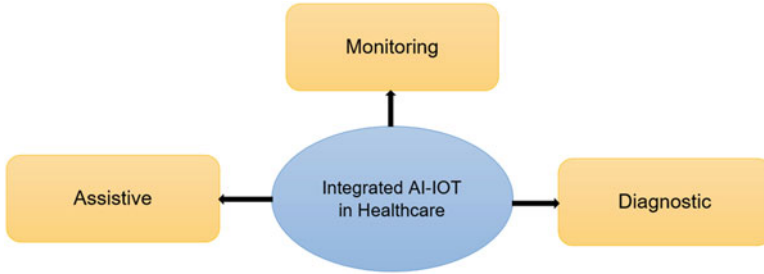
Fig. 1 Role of IoT in the healthcare sector [5]

diseases at once, but it can at least make healthcare more affordable and accessible, as we have the Aarogya Setu app for protecting ourselves from COVID-19 [3]. It has made it possible for people to provide and receive healthcare services across a series of interconnected networks and IoT devices, i.e., it has shifted the routines of medical check-ups from a hospital-centric to a patient-centric environment” [4]. With the help of IoT in the healthcare sector, there are unparalleled benefits that could improve the quality and efficiency of treatments and accordingly the health of patients. Healthcare practitioners can collect data using IoT devices such as smart pills, wearable monitors, and sensors. It has evolved the way stakeholders currently interact and will continue to streamline the processes involved in frontline healthcare work” [5].

As shown in Fig. 1, the patient’s body has been fixed by various sensors like blood pressure sensor, patient position sensor, pulse and oxygen sensor, electromyography sensor, etc. These sensors collect the data of the particular area where they have been attached. The collected data is then transferred to the cloud where it is stored via PDA, smartphones, Bluetooth, Zigbee, or Wi-Fi. The cloud allows the e-storage of the patient’s record, which includes images, documents, and videos. It enables better collaboration of data and transfers it to medical representatives via various network connections so that the medical team can easily reach the patient and can effectively diagnose them. The main function of the cloud is to provide analysis of the data so that both the sender (patient) and receiver (doctors or nurses) can get the maximum benefit of an IoT infrastructure.

### 1.1 IoT and AI in Healthcare

The Internet of Things and artificial intelligence, which includes machine and deep learning, have been widely applied in physical health. Machine and deep learning are strategies for learning from the precedents and experiences without being expressly modified [48]. The systems under IoT are a collection of interconnected



**Fig. 2** Bridge between IoT and AI in the healthcare sector [9]

devices that perform predictive analysis, diagnosis, remote monitoring, preventive analysis, and surgeries [6]. Machine and deep learning can determine whether the patient is in an abnormal state or not, and if there are any abnormalities, such as low heart rate or increased temperature, immediate relief measures will be triggered with the help of machine learning. Machine and deep learning methods are also important in predicting new attacks because they can intelligently predict future unknown attacks by learning from known ones, thereby providing an effective and secure system.

Figure 2 represents the roles of machine and deep learning algorithms in IoT-enabled healthcare, which are briefly described as follows:

**Assistive** Artificial intelligence along with IoT has powered assistive technologies with significant benefits for people, particularly those with disabilities. Its main purpose is to maintain and improve an individual's functioning.

**Monitoring** The ability to monitor patients using artificial intelligence allows to communicate information to physicians to determine whether the disease is there or not. For this, a wearable device is used, which constantly monitors the patients and keeps on notifying the medical representatives.

**Diagnostic** The use of artificial intelligence can help to reduce medical costs by improving diagnostic accuracy and assuming better predictions in treatment plans to keep patients healthy.

The chapter is organized into different sections: Sections 1 expresses the motivation for using machine learning and deep learning techniques in IoT-enabled healthcare, along with the advantages and disadvantages of IoT. Section 2 is a background study where we discussed the framework of IoT in healthcare, how IoT works in healthcare systems, and applications of IoT in healthcare devices. Section 3 is all about the reported part, which focuses on the machine and deep learning techniques used by the researchers in their proposed methodology, along with other optimization techniques. Section 4 highlights the work done by the researchers in tabular form. Finally, Sect. 6 concludes the chapter by discussing the future scope of IoT in healthcare devices.

## 2 Motivation

We all know that IoT has been in trend since ages and it has played an important role in every domain, whether it is related to customer applications, industrial applications, commercial applications, business applications, etc. Likewise, it has also done a desirable work in the healthcare sector by providing accurate collection of patient's data, which subsequently reduces error, allowing connected home care facilities, improving diagnosis accuracy, continuously monitoring the patient's health, providing the best treatment process to patients, reminding the patients if their medication has not been taken on time, reducing costly visits to the doctor and hospital admissions, providing quick access to doctors, providing real-time location system for hospitals and other medical facilities, and enabling remote medical assistance, and it can also be used for research purposes, working on massive amounts of patient data. But, simultaneously, IoT has also become challenging due to its shortcomings, such as lack of memory to store massive data repositories, threat to private data security, unauthorized access to the centralized system, risk of failure in hardware affecting the operation of sensors, high cost of implementation in hospitals or homes, faults in data accuracy, etc.

Thus, keeping the above facts in consideration, researchers have used various methodologies that are based on machine and deep learning to incorporate and improve IoT in healthcare, as both machine and deep learning are important for providing secure communication between devices and security-based intelligence systems, allowing the system to accurately predict the disease for a particular patient, monitoring the health condition of the patient, providing better data storage and processing, enabling the extraction of relevant information from the huge amount of data stored, providing reliable data, and resolving the huge complex data in less time.

Hence, the primary goal of this research is to highlight the contributions made by the researchers to provide us with guidance about the role and importance of IoT in the healthcare sector using abovementioned algorithms.

## 3 Background Study

The background study of IoT-based healthcare defines the framework of IoT in healthcare and the operation of IoT in healthcare that depicts its architecture, followed by its applications and need in hospitals.

### 3.1 Framework of IoT in Healthcare

A framework is a blueprint that provides an outline to conduct the research and describes why the research problem under study exists. Thus, to provide such blueprint, the framework of IoT enabled in healthcare is represented in the form of certain blocks, as shown in Fig. 3, which are explained in a nutshell as follows [2]:

**Human Input** The main IoT input tools are network and sensor. These devices take the patient’s input from multiple sensors embedded in wearable devices. These input devices enable to connect other things or services.

**Visualization Interface** On the basis of the input taken, either drawings or images or animations are made to communicate the message because it is an effective way to communicate the patient’s report in a concise manner.

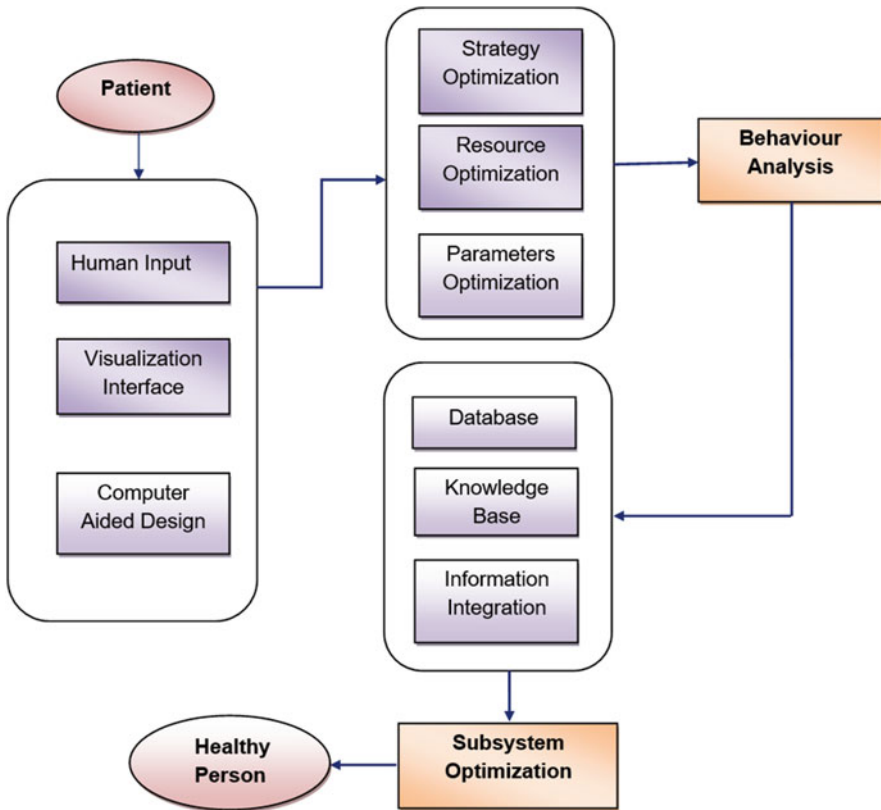


Fig. 3 Framework of IoT in healthcare devices [2]

**Computer-Aided Design** It is used for the modifications, creation, analysis, or optimization of a design that has been taken as an input from the VI. CAD software is used to enhance the productivity of the designer and improve the quality of the design and communication through documentation.

**Resource Optimization** The resource optimization methods improve the distribution and supply of healthcare providers to maximize service coverage, minimize travel, and maximize health.

**Strategy Optimization** Strategic planning in healthcare involves outlining actionable steps to achieve specific goals. It includes providing proper nutrition, safe drinking water, basic sanitation, immunization, etc.

**Behavioral Analysis** Behavioral analysis is a natural science that studies the behavior of individuals. Applied behavioral analysis applies the scientific principles of behavior analysis to treat patients with problematic behaviors who may be suffering from developmental difficulties, head trauma, neurological diseases, or other mental issues.

**Database** The information collected from the behavioral analysis of the patient is stored in the cloud database for further processing.

**Knowledge Base** It is the end product of collecting and organizing information into a useful form through a process called knowledge management. Thus, knowledge management is used to collect the information, whereas knowledge base software is used to create, manage, and deliver that information”[10].

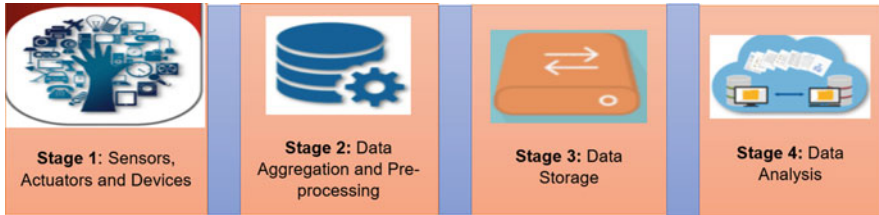
**Information Integration** It is the method of merging processed information with differing conceptual, contextual, and typographical representations. The integration of health information technology into primary care includes electronic methods that are used to manage information for individual patients and groups of patients.

**Subsystem Optimization** After having the final output, the subsystem optimization technique is used to focus on any one component whose changes can improve the rest of the defects, thereby converting the patient to a healthy one.

### ***3.2 How IOT Works in Healthcare***

“The rise of IoT-enabled healthcare devices creates enormous opportunity. Furthermore, the massive volume of data created by these linked devices has the potential to revolutionize healthcare. The Internet of Things features a four-step design that resembles stages in a process, as seen in Fig. 4. Each of the four steps is related in such a way that data is recorded or processed at one level and then used to generate value at the subsequent step. Integrating values throughout the process fosters intuition and results in innovative commercial opportunities [11].





**Fig. 4** The four stages of IoT solutions [11]

*Step 1:* The initial stage entails the transmission of networked gadgets, which may include sensors, actuators, displays, finders, and camera frameworks. These devices collect data.

*Step 2:* Typically, data acquired from sensors and various devices is in a simple structure, which must be collected and converted to a more advanced structure for additional data handling.

*Step 3:* After the data is digitized and collected, it is preprocessed, normalized, and transferred to the server farm or cloud.

*Step 4:* The final data is supervised and investigated at the appropriate level. When applied to this data, advanced analytics reveals significant business insights for a powerful dynamic.

The Internet of Things is reclassifying medical services by ensuring greater consideration, improved therapy outcomes, and reduced costs for patients, as well as enhanced cycles and work processes, improved execution, and a better patient experience for medical service providers, whereas the Internet of Medical Things is a connected infrastructure of medical devices, software applications, and health services. It is a wave of sensor-based tools that includes wearable and standalone devices for remote patient monitoring [12]. The Internet of Medical Things has grown as the number of connected medical devices that generate, collect, analyze, or transmit health data or images has increased. It connects to healthcare provider networks to transmit data to either a cloud repository or internal servers. It has the potential to accurately diagnose, show fewer mistakes, and provide low-cost care. While combined with smartphone applications, the technology allows patients to send their health information to doctors to survive from the diseases and prevent chronic illnesses. The Internet of Medical Things not only helps to improve the experience of the patient by eliminating the need for in-person medical visits but also helps to reduce costs”[14]. The Internet of Medical Things is an important component of the digital transformation in the field of healthcare because it allows new business models to incorporate and enable changes in work processes, improves productivity, reduces costs, and also enhances customer experiences. We all know that wearable and mobile apps support fitness, health education, symptom tracking, and collaborative disease management and care coordination. The healthcare sector rapidly adopted various IoT solutions by creating the Internet of Medical Things. Devices like heart rate monitors and pacemakers collect and send patient data to

healthcare providers via various networks for monitoring, analysis, and remote configuration [15]. Integration of IoT in medical devices navigates the patient's health and alerts medical experts prior to the occurrence of any infection, with its main focus of minimizing the time of project submission and cost [16]. The significant points of interest of IoT in medical services include the following [8, 12, 49]:

- *Cost Reduction*: IoT enables continuous understanding observation, thereby reducing unnecessary visits to specialists, emergency clinic stays, and reaffirmations.
- *Improved Treatment*: It enables doctors to settle on proof-based educated choices and brings supreme straightforwardness.
- *Quicker Disease Diagnosis*: Continuous understanding checking and ongoing information helps in diagnosing ailments at an early phase or even before the malady manifests itself.
- *Proactive Treatment*: Continuous well-being monitoring opens the entryways for giving proactive clinical treatment.
- *Medications and Equipment Management*: Management of medications and clinical hardware is a significant test in the medical care industry. Through associated gadgets, these are overseen and used productively with reduced expenses.
- *Mistake Reduction*: Data generated through IoT gadgets help in powerful dynamic as well as guarantee smooth medical care tasks with reduced errors, waste, and framework costs. The IoT in medical care is not without challenges. IoT-enabled associated gadgets collect massive amounts of information, including data, giving rise to concerns about information security. Actualizing well-suited safety efforts is critical. IoT investigates new elements of patient consideration through constant well-being checking and access to patients' well-being information. This information is a goldmine for medical service partners to improve patient's well-being and encounters while making income openings and improving medical service activities. Being prepared to outfit this computerized force would end up being the differentiator in an inexorably associated world"[12].

### 3.3 Need of IoT in Healthcare Devices

"Prior to the Internet of Things, patients' collaborations with specialists were restricted to in-person visits, as well as teleconferences and text messages. There was no way for chance specialists or medical clinics constantly monitor patients' well-being and make recommendations as needed. Internet of Things (IoT)-enabled gadgets have made remote testing in the medical care field possible, releasing the possibility to keep patients safe and sound and engaging doctors to deliver exceptional care. It has additionally expanded patient commitment and fulfillment

as associations with specialists have become simpler and more proficient. Moreover, remote monitoring of patient's well-being helps in reducing the length of time spent in an emergency clinic and forestalls reconfirmations. IoT also has a significant impact on reducing medical service costs and improving therapy results"[13]. IoT is without a doubt changing the medical care industry by rethinking the role of gadgets and individuals in conveying medical care arrangements. IoT has applications in medical services that benefit patients, families, doctors, emergency clinics, and insurance agencies [15].

- *IoT for Patients* – Wearable devices, similar to wellness groups, and other remotely associated gadgets give patients access to personalized care. These gadgets can be programmed to remind you of carbohydrate levels, practice checks, arrangements, circulatory strain varieties, and considerably more. IoT has transformed people, particularly old patients, by enabling continuous monitoring of well-being conditions. This majorly affects individuals living alone and their families. On any unsettling influence or changes in the normal exercises of an individual, the ready instrument sends signals to relatives and concerned health providers"[11].
- *IoT for Medical Experts* – Using smart devices and other home monitoring equipment incorporated with the Internet of Things, doctors can diagnose patients' well-being more efficiently. IoT enables medical representatives to be more vigilant and linked with patients energetically. Data provided by the Internet of Things can assist medical experts provide good diagnosis measures to patients, along with normal results [11].
- *IoT for Health Center* – Apart from analyzing patients' health, there are a number of zones where IoT devices are exceptionally important in emergency clinics. IoT-based devices with body sensors are used for hardware equipments like wheelchairs, defibrillators, nebulizers, oxygen siphons, and other monitoring equipment. Organization of clinical staff in various areas can likewise be investigated constantly" [12]. The spread of diseases is a major concern for patients in medical clinics. The Internet of Things enabled the devices to keep patients away from getting contaminated.
- *IoT for Health Insurance Companies* – There are various open doors for well-being guarantors with IoT-associated smart gadgets. Insurance agencies can use information gathered through well-being monitoring gadgets for endorsing and claims tasks"[9]. This information will empower them to distinguish misrepresentation guarantees and recognize possibilities for endorsing. The endorsing, estimating, claims handling, and risk evaluation measures of IoT gadgets gain trust among safety net providers and clients. Guarantors may offer impetuses to their clients for utilizing and sharing well-being information generated by IoT gadgets. They can compensate clients for utilizing IoT gadgets to monitor their standard exercises and adherence to treatment plans and preventive health measures. This will assist backup plans with decreasing cases essentially. IoT gadgets can likewise empower insurance agencies to approve claims based on the information gathered by these gadgets"[13].

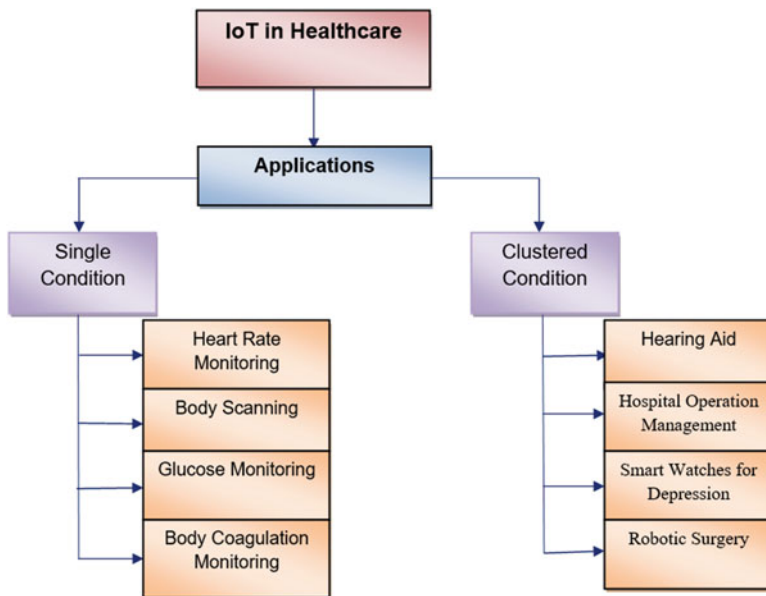


Fig. 5 Applications of IoT in healthcare devices [2]

### 3.4 *Internet of Things in Healthcare: Applications*

By collaborating with the Internet of Things, various problems can be solved. The efficiency level of medication and diagnosis can be improved by various IoT-based solutions. A few examples of IoT applications in the healthcare sector are depicted in Fig. 5 under single and clustered conditions.

Table 1 presents the numerous ways in which IoT-enabled devices can be applied to various devices and the significance of these things. Every component has a specific use case explanation detailing how it helps a healthcare system, not just a specific patient.

## 4 Reported Work

As far as the topic is concerned, the IoT appears to be thriving in the field of health sector by incorporating it into various healthcare services like tracking of doctors, medical equipments, alerts regarding the patient's condition, remote medical assistance, and many more [15]. In a nutshell, IoT enables healthcare professionals to be connected with patients more proactively, though it also deals with certain issues like data security, privacy, data overloading, and cost of implementation [17]. But keeping in view its best side in the health sector, various researchers have done lots

**Table 1** Applications of IoT in healthcare

Application	Description
“Heart rate monitoring	IoT-based applications are useful to detect heartbeat and pulse rate so that the risk factor can be reduced. A sensor connected device sends the data to the cloud, which helps doctors monitor the patient’s heart from any nook of the world [5].
Body scanning	The smart body scanner is useful for tracking body changes that indicate other parameters, followed by comparison between previous and recent results [7].
Glucose monitoring	It is well understood that insulin regulates the level of glucose in the blood, and if the pancreas produces little amount of insulin, blood sugar levels can fluctuate in our bodies. Thus, IoT applications embedded with wearable body sensors constantly monitor and send data about our body’s sugar level, which in turn minimizes the risk of diabetes in patients [10].
Body coagulation testing	A blood clot has an important role in the human body. Information of blood clots is important for the recovery of multiple diseases like diabetes, stroke, etc. In healthcare, the Internet of Things monitors the blood coagulation level on a regular basis to keep track of the patient’s activity [5].
Hearing aid	Hearing aid IoT helps in hearing sound in a noisy environment. Even people can listen in on multiple interactions at the same time [5].
Hospital operation management	The hospital is a crowded place where lots of people work. Occasionally, medical representatives are so busy that they can’t observe multiple patients simultaneously and so on. Such problems are accumulated by the IoT by reducing the daily cost of medical equipment, providing the present location of the required equipment to save the time, and monitoring the tie complexity of sending the notifications to patients [3].
Smart watches for depression	Every year there are so many people who become the prey of depression, and smart watches can assist them by navigating and advising the patient on how to deal with depression [4].
Mechanized operation	As we all know, the complexity of human healthcare is increasing day by day, and in order to operate more accurately, surgeons rely on automatic or self-regulating machines where long-term operation can be performed [2, 7].

of work to promote its growth efficiently and effectively, out of which two major applications of AI have been discussed that have played seminal role in IoT.

#### ***4.1 IOT in Healthcare Using Machine Learning***

The field of machine learning is growing steadily along with the growth of IoT. There are millions of IoT devices around the world that collect huge amount of data, which is then sent to machines via the Internet, allowing them to learn from the data

and create better machine learning models. Many researchers have proposed various models to use machine learning algorithm in IoT healthcare systems.

*Bholwal, A.* [18] has presented the design based on machine learning algorithms and cloud to provide better operation of IoT in healthcare systems. The author has used different sensors to assess the physical condition of the patients, LPWAN to monitor critical situations, and a smartphone connected to both the sensors and low-power wide area networks to display and send messages. These message signals are then uploaded to the cloud via a gateway, which helps the patients to communicate with healthcare professionals. Decision tree has been used at the central node, which sends signals from the sensor to either the smartphone or the LPWAN. Few optimized machine learning algorithms have been enabled in the cloud to monitor patient's progress. Besides this, the author has also mentioned the security issue, for which an intruder detection system has been incorporated into the cloud. *Sathya, M. et al.* [19] have also designed a four-layered protocol system: a physical layer, which is embedded with sensors and transmitters; a network layer, which is responsible for transmitting signals from sensors to cloudlets; a middleware layer, which stores data in the cloud; and an application layer, where analytics and diagnosis are performed using machine learning algorithms to correlate sensor parameters and clinical data. *Reddy, S. et al.* [20] have worked on a PIC microcontroller that is connected to five sensors, including heartbeat, temperature, blood pressure, blood glucose level, and MEMS. The authors used machine learning, specifically the KNN algorithm, to perform classification of diseases on the values obtained from sensors, allowing them to assess the condition of the patients. *Priyadharshan, J. et al.* [21] proposed a system that is based on sensors that collect the data and micro controllers that process it. The sensors are connected to the Raspberry PI, which is a central server, via GPIO pins or MCP3008 analog to digital converter. The processed data is stored in the cloud for analysis. The KNN classifier has been incorporated to classify the patient's health status. Three algorithms of machine learning have been used on the same dataset: decision tree, Naïve Bayes, and support-vector machine algorithm, with decision tree having accuracy higher than the other two. *Yadav, S. and Jadhav, S.* [22] worked on real-time healthcare dataset that has been generated from various sensors such as ECG sensor, temperature sensor, etc., which are connected to Raspberry Pi and is then sent to a microcontroller. Raspberry Pi B<sup>+</sup> is used to store data in the cloud. Algorithms like probabilistic fuzzy random forest, classification using linear regression, and Q-learning algorithm have been applied to analyze the processed data, with fuzzy random forest proving to be the best in accuracy. *Panda, S. and Panda, G.* [23] worked on two datasets, i.e., LSVT voice data and CNAE-9 dataset, and used random forest, decision tree, and Naïve Bayes as classifiers. To extract the features from raw data, principal component analysis has been used, on which the abovementioned classifiers are applied. F1 score is also taken into consideration to evaluate the performance measure. *Ismail, A. et al.* [24] proposed a speech recognition-based methodology to train the system based on certain commands, with the help of which patients, the elderly and the disabled, can execute their tasks easily without anyone's support. Machine learning algorithm,

i.e., support-vector machine along with DTW, is used to match the voice commands and detect its semantics.

## ***4.2 IoT in Healthcare Using Deep Learning***

When it comes to solving complex problems, deep learning has always been a savior. Deep learning is assisting medical professionals to discover hidden opportunities in data and to serve the healthcare industry in a better way. Thus, multiple deep learning technologies that have been used by researchers in IoT for healthcare are described briefly below.

*Jeyaraj, P. and Nadar, E. [25]* proposed a learning architecture based on a monitoring unit that includes RIO processor, processing unit, visualization and storage unit that uses an IoT gateway, and learning unit for signal feature prediction and notification module. The authors had applied a deep neural network to extract the features from the acquired signal to compute a scoring function for constraint-based signal and a stochastic descent method to determine the abnormality for the acquired signal. *Obinikpo, A. and Kantarci, B. [26]* had discussed about the deep learning methods on medical sensory datasets for e-health applications such as deep feedforward neural networks, autoencoder, convolutional neural network, deep belief network, and Boltzmann machine. *Ismail, W. et al. [27]* proposed a CNN-based model to discover the association between positively and negatively correlated factors. Its complexity is directly proportional to the number of inputs. The two most important techniques used in this research are principal component analysis and factor analysis. *Mao, S, et al. [28]* designed the AutoTag system, which consists of a recurrent variational autoencoder model with RFID tags and signal extraction, calibration, respiration monitoring modules. *Rajan, J. et al. [29]* designed an architecture that has a MIDAS dataset to detect ROI in an IoT healthcare system. They applied a multilayer supervised network for learning the data from the input set. This architecture is mainly designed for cancer detection. *Young, F. et al. [30]* proposed a smart glass device which is based on a microcontroller to provide real-time information. Convolutional neural network-based image classifier is used to identify patterns and clusters. A deep learning model, i.e., Inception v4, with transfer learning is used to detect and recognize data.

## ***4.3 IoT in Healthcare Using Optimization Techniques***

There are also few techniques other than machine learning and deep learning used by the researchers, which are summarized below:

*Li, C. et al. [31]* proposed an architecture which is based on sensing layer, transport layer, and application layer. They worked with the sampling frequency of the ECG signals and used four modes of operation to monitor the system,

such as real-time transmission for continuous data, continuous transmission in all periods, even triggered transmission, and at last transmission on patient's demand. The authors called their system as "pervasive monitoring system." *Zhu, H. et al.* [32] designed a system that consists of virtual reaction chambers, fully integrated PCR, and a silicon chip made up of micro-electromechanical system technology. The data from the PCR system are downloaded and automatically sent via LTE network to a dedicated location monitoring the disease outbreak. *Soufiene, B. et al.* [33] presented their IoT architecture based on the PEERP, which includes medical sensors, personal aggregators, and healthcare services. The PEERP is divided in to three phases: initial phase, next-hop selection phase, and forwarding phase. The comparison between the ATTEMPT and PEERP has also been shown in the paper. *Kumar, S. and Majumder, D.* [34] used multiple sensors like SPO2 sensor, ECG sensor, EEG sensor, temperature sensor, and EMG sensor, MQTT/COAP as IOT protocol, and Hadoop and Tensorflow as back-end servers. *Banka, S. et al.* [35] proposed an automatic system based on Raspberry Pi to which all sensors and power supplies are connected. It has the capability to monitor the patient's body temperature, heart rate, body movements, etc. and also the status of the patient's disease. They used health monitoring services, emergency alert section, and health status prediction system in their architecture.

## 5 Comparative Analysis

Table 2 represents the work of various researchers in the field of IoT-embedded healthcare, along with the different techniques used, which are mostly based on machine and deep learning, multiple datasets [47], and the results achieved by them in succinct form.

From Table 2, it has been observed that researchers have embedded various IoT components in healthcare and have applied patient's data to it that are collected from various datasets. They have used multiple techniques that have shown better accuracies, but it has been determined that deep neural networks produce the best accuracy when compared to machine learning techniques because machine learning has a high error susceptibility, cannot work with large datasets, and sometimes fails to interpret the results efficiently.

## 6 Conclusion and Future Directions

Researchers have explored various technological ways to enhance the Internet of Things services in healthcare. This chapter defines motivation along with framework of the Internet of Things in healthcare. It also contains the importance and fruitful benefits of IoT in the healthcare system along with its shortcomings. The chapter offers a broad overview of how recent and ongoing advances in sensors, devices,



**Table 2** Tabular representation of the methodologies used in IoT-based health services

Authors	IOT-enabled healthcare component	Dataset	Techniques	Reported results
K Reddy, S. et.al [20]	Sensors, PIC microcontroller	ThingSpeak database	KNN	Accuracy = 78.43
Priyadarshan, D. et.al [21]	Sensors, Raspberry Pi	Real-time patient's data	KNN classifier, NB, DST, SVM	Accuracy: NB = 70 DST = 70-80 SVM = 60-70
Yadhav, S. Jadhav, S. [22]	Six sensors, Raspberry Pi, GSM module, MAX232	Synthetic data and real-time patient data	Fuzzy random forest, linear regression, Q-learning	Accuracy: FRF = 80-100 LR = 80 QL = 80
Ismail, A. et.al [24]	Raspberry Pi, smart devices	Training speech template	Support-vector machine, dynamic timing machine	Accuracy: SVM = 79 SVM with DTW = 97
Jeyaraj, P. Nadar, E. [25]	NI-myRIO, sensor, Xilinx FPGA processor	Signal dataset	DNN, stochastic descent method	Average accuracy = 97.2
Mao, S et.al [28].	RFID, RSSI, AutoTag system	RFID tags	Autoencoder, LSTM	Accuracy = 88
Young, F. et.al [30]	ESP8266 board, MFCC	Sound classification from real-world dataset	Inception V4 deep network, VGG, transfer learning	Accuracy: Inception v4 = 82 VGG = 70
Sood, S. Mahajan, I [36]	Wearable IoT sensor	CHV-based dataset of patient	FCM classifier, SNA graph, ORI,	Specificity: FCM 1.4 = 86.7 FCM 1.6 = 87.3 FCM 1.8 = 88.4
Gondalia, A. [37]	Sensor, Zigbee, LoRaWAN, microcontroller, WBAN	Data collected of soldiers' health from the war zone	K-means clustering	Graph between temperature, humidity, and heartbeat
Amin, S. et al. [38]	EEG sensor, LoWPAN, Zigbee	TUH dataset	CNN, AlexNet, VGG, SVM	Accuracy = 86

(continued)

Table 2 (continued)

Authors	IOT-enabled healthcare component	Dataset	Techniques	Reported results
Karnatapu, H [39]	Smart devices, sensor	Patient's real-time-based data	CheXNet algorithm	It is effective but delayed because of kits
Hamza, R. et al. [40]	Sensors, smart devices, communication bandwidth	WCE dataset	Encryption, decryption, PRNG, algorithm	Encryption = 970 kb/sec
Mani, N. et.al [41]	Smart devices, sensors	Real-time dataset	Fog computing,	Lack of security, provides better information
Raj, C. et al. [42]	Pulse oximeter Arduino shield, AVR Atmega 328P, sensors	Data is inherited from sensor node	Telemedicine, LAB VIEW	Accuracy: ECG = 76
Kakkar, A et al. [43]	Sensors, RFID readers, WBLC, smart system	Village patient's dataset	GCSK, RFID, cloud service, E-governance	Treats critical healthcare requirements
Albeshar, A [44].	Smart devices, sensors, wearable devices	Louisville dataset	AAL, La Roche-Posay UV sensor, NFC	Presented the optimized services of IoT in healthcare
Baker, S. et al. [45]	Body sensor networks, wearable sensors, SPHERE	Previous patient's dataset	Machine learning algorithms, cloud services	Accuracy = 87.9
Dewangan, K, Mishra, M [46]	WBAN, BSN, smart devices	Real-time dataset	RFID, ECDH, CoAP, MQTT	Improved the security issues by incorporating the protocols into the mechanism
Sathya, M. et al. [19]	Sensors, transmitters	Data inherited from sensor node	Cloudlet, ML algorithms	Cloud-based IoT has been used to overcome the connectivity issue data between the different cloud environments
Zhu, H. et al. [32]	Real time PCR, PCB	Amplicon dataset	MEMS, cloud service, ELISA,	Boltzmann curve: Mean 81.98 SD = 0.16

etc. have made the lives of patients easier and more affordable in terms of medicines and health services. It studies the impact of technologies such as machine learning and deep learning in IoT applications in the healthcare sector. In addition, the chapter also provides detailed research activities performed by various researchers to showcase the impact of using optimization techniques of IoT in healthcare. The systematic literature survey highlights the key concepts of research in technologies such as IoT and artificial intelligence, including the comparative analysis that has been shown in a tabular form where each column defines the dataset, techniques, and IoT components used by the researchers along with its remarks. Even though IoT has infinite advantages, its challenges and limitations can hamper the growth of IoT especially in the healthcare sector. Thus, as part of future work, it is necessary to work on these shortcomings, such as security issues, privacy protection, malware attacks, outdated hardware devices, etc., so that they never impede the process and provide smooth communication and data transfer between patients and medical representatives.

## References

1. H. Malik, M. Alam, Y. Moullec, A. Kuusik, Narrow band IoT performance analysis for healthcare applications. *Healthcare Appl.*, 1077–1083 (2018)
2. S. Islam, D. Kwak, H. Kabir, M. Hossain, K. Kwak, The internet of things for healthcare: A comprehensive survey. *Internet of Things* **3**, 678–708 (2015)
3. S. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, J. Isoaba, Performance analysis of end-to-end security schemes in healthcare IoT. *Netw. Secur.* **432**, 439 (2018)
4. D. Dziak, B. Jachimczyk, W. Kulesza, IoT based information system for healthcare application: Design methodology approach. *Appl. Sci.* **7**, 2–26 (2017)
5. C. Fonseca, D. Mendes, M. Lopes, A. Romao, P. Parreira, Deep learning and IoT to assist multimorbidity home based healthcare. *J. Health Med. Inf.* **8**, 1–4 (2017)
6. Z. Alansari, S. Soomro, M. Belgaum, S. Shamsriband, The rise of internet of things in big healthcare data. *Internet of things in healthcare* **564**, 675–685 (2018)
7. M. Kang, A study on the continuing usage of IoT based healthcare wearable devices. *Blue Eyes Intell. Eng. Sci.* **8**, 74–76 (2019)
8. H. Zakaria, N. Bakar, N. Hassan, S. Yacob, IoT security risk management model for secured practice in healthcare environment. *Procedia Comput. Sci.* **161**, 1241–1248 (2019)
9. S. Pinto, J. Cabral, T. Gomes, We care: An IoT based healthcare system for elderly people. *Healthcare Syst.*, 1378–1383 (2017)
10. P. Kumar, S. Lokesh, R. Varatharian, G. Babu, P. Parthasarathy, Cloud and IoT based disease prediction and diagnosis system for healthcare using fuzzy neural classifier. *Futur. Gener. Syst.* **86**, 527–534 (2018)
11. P. Shakeel, S. Baskar, V.R. Dhulipala, S. Mishra, M. Jaber, Maintaining security and privacy in healthcare system using learning based deep Q networks. *J. Med. Syst.* **42**, 1–10 (2018)
12. M. Elhoseny, R. Gonzalez, O. Elnasr, S. Shawkat, N. Arunkumar, A. Farouk, Secure medical data transmission model for IoT based healthcare systems. *Med. Things* **6**, 20596–20608 (2018)
13. P. Kumar, U. Gandhi, A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. In: 2018, vol. 65 (Elsevier, 2018), pp. 222–235
14. P. Verma, S. Sood, Cloud-centric IoT based disease diagnosis healthcare framework. *J. Parallel Distrib. Comput.* **116**, 27–38 (2018)

15. A. Qayyum, J. Qadir, M. Bilal, A. Fuqaha, Secure and robust machine learning for healthcare: A survey. *Biomed. Eng.*, 1–22 (2020)
16. L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, M. Vento, Trends in IoT based solutions for healthcare: Moving AI to the edge. *Pattern Recogn. Lett.* **135**, 346–353 (2020)
17. Y. Kumar, K. Sood, S. Kaul, R. Vasuja, Big data analytics and its benefits in healthcare, in *Big Data Analytics in Healthcare*, Studies in Big Data, vol. 66, (Springer, Cham, 2020), pp. 2013–2235
18. A. Bholwal, Extensive study Of IoT in healthcare based on machine learning and cloud. *Innov. Eng. Technol.* **12**, 014–018 (2019)
19. M. Sathya, S. Madhan, K. Jayanthi, Internet of things based health monitoring system and challenges. *Sci. Pubco* **7**, 175–178 (2018)
20. S. Reddy, R. Sidaarth, S. Reddy, R. Shettar, IoT based health monitoring system using machine learning. *Res. Innov. Ideas* **5**, 381–386 (2019)
21. D. Priyadarshan, K. Sanjay, S. Kathiresan, K. Karthik, K. Prasath, Patient health monitoring using IoT with machine learning. *Eng. Technol.* **6**, 7514–7520 (2019)
22. S. Yadav, S. Jadhav, Machine learning algorithm for disease prediction using IoT environment. *Blue Eyes Intell. Eng. Sci. Publ.* **8**, 4303–4307 (2019)
23. S. Panda, G. Panda, Intelligent classification of IoT traffic in healthcare using machine learning techniques. *Control Autom. Robot.*, 581–585 (2020)
24. A. Ismail, S. Abdlerazak, M. Ibrahim, and E. Henway, Development of smart healthcare system based on speech recognition using support vector machine and dynamic time wrapping, in *Pattern Recognition*, vol. 12, Sustainability, 2020, pp. 1–15
25. P. Jeyaraj, E. Nadar, Smart monitor: Patient monitoring system for IoT- based healthcare system using deep learning. *Electron. Telecommun.*, 1–8 (2019)
26. A. Obnikipo, B. Kantarci, Big sensed data meets deep learning for smarter healthcare in smart cities. *Sensor Actuator Netw.* **6**, 1–22 (2017)
27. W. Ismail, M. Hassan, H. Alsalamah, G. Fortino, CNN- based health model for regular health factors analysis in Internet of Medical things environment. *Deep Learn Algorithms Internet of Medical Things* **8**, 52541–52549 (2020)
28. C. Yang, X. Wang, S. Mao, AutoTag: recurrent variational autoencoder for unsupervised apnea detection with RFID tags. *Deep Learn.*, 1–7 (2018)
29. J. Rajan, S. Rajan, R. Martis, B. Panigarhi, Fog computing employed computer aided cancer classification system using deep neural network in Internet of Things based healthcare system. *Image Signal Process.* **34**, 1–10 (2020)
30. F. Young, R. Jiang, H. Liu, C. Wall, A deep learning based wearable healthcare IoT device for AI enabled hearing assistance automation. *Mach. Learn. Comput.*, 1–9 (2020)
31. C. Li, X. Hu, L. Zhang, The IoT based heart disease monitoring system for pervasive healthcare service. *Knowl. Based Intell. Inf.* **112**, 2328–2334 (2017)
32. H. Zhu, X. Liu, H. Zhang, T. Teply, Y. Xu, H. Chang, A. Qian, Y. Lei, A. Niculescu, C. Iliesu, P. Neuzil, IoT PCR for pandemic disease detection and its spread monitoring. *Sensors Actuators B Chem.* **303**, 1–7 (2019)
33. B. Soufiene, A. Bahattab, A. Trad, H. Youssef, PEERP: An priority based energy efficient routing protocol for reliable data transmission in healthcare using IoT. *Procedia Comput. Sci.* **175**, 373–378 (2020)
34. S. Kumar, D. Majumder, Healthcare solution based on machine learning applications in IOT and edge computing. *Pure Appl. Math.* **119**, 1473–1483 (2018)
35. S. Banka, I. Madan, S. Saranya, Smart healthcare monitoring using IoT. *Res. India* **13**, 11984–11989 (2018)
36. S. Sood, I. Mahajan, Wearable IoT sensor based healthcare system for identifying and controlling chikungunya virus. *Comput. Ind.* **91**, 33–44 (2017)
37. A. Gondalia, D. Dixit, S. Parashat, V. Raghava, A. Sengupta, IoT based healthcare monitoring system for war soldiers using machine learning. *Procedia Comput. Sci.* **133**, 1005–1013 (2018)

38. S. Amin, M. Hossain, G. Muhammad, M. Aluhussein, A. Rahman, Cognitive Smart Healthcare for Pathology Detection and Monitoring. *Artif. Intell. Cogn. Comput. Commun. Netw.* **7**, 10745–10753 (2019)
39. H. Karnatapu, An approach to monitor coronavirus using IoT and machine learning, in *Virology*, Research Gate, 2020, pp. 1–16
40. R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, A Privacy Preserving cryptosystem for IoT E-Healthcare. *Information Sciences*, 1–18 (2019)
41. N. Mani, A. Singh, S. Nimmagadda, An IoT guided healthcare monitoring system for managing real-time notifications by fog computing services. *Procedia Computer Science* **167**, 850–859 (2020)
42. C. Raj, C. Jain, and W. Arif, HEMAN: Health monitoring and nous, in *Remote telemedicine*, IEEE, 2017, pp. 2115–2119
43. A. Kakkar, S. Shaurya, An IoT equipped hospital model: A New approach for E-governance healthcare framework. *Medical Research and Health Sciences* **8**, 36–42 (2019)
44. A. Albeshier, IoT in Healthcare: Recent advances in the development of smart cyber- physical ubiquitous environments. *Network Security* **19**, 181–186 (2019)
45. S. Baker, W. Xiang, Internet of Things for smart healthcare: Technologies, challenges and opportunities. *Smart Technologies*, 1–25 (2018)
46. K. Dewangan, M. Mishra, Internet of Things for healthcare: A review. *Management and Technology* **8**, 526–534 (2018)
47. Y. Kumar, M. Mahajan, Intelligent behavior of fog computing with IOT for healthcare system. *Int. J. Sci. Technol. Res.* **8**(7), 674–679 (2019)
48. I. More, Y. Singla, S. Verma, U. Ghosh, J. Rodrigues, A. Hosen, Security assured CNN based model for reconstruction of medical images on the internet of healthcare things. *IEEE Access* **8**, 126333–126346 (2020)
49. U. Ghosh, D. Rawat, R. Datta, A. Pathan, *Internet of Things and Secure Smart Environments: Successes and Pitfalls* (CRC Press, Boca Raton, 2020), pp. 1–10

# Network Protocols for the Internet of Health Things



Trisha Das Mou and Gautam Srivastava 

## 1 Introduction

The Internet of Things (IoT) was initiated to connect devices to the Internet and to each other. Beyond machine-to-machine communication, the state-of-the-art technology of IoT emerges as a megatrend by merging WSN devices, systems, and services [2]. An interrelation chain is considered, as these connections create an influence on the entire business space. The interesting matter is that we can identify powerful, smart projects and gadgets in existing web frameworks that have a wide range of benefits. Essentially, the wireless communication system is the base of the IoT model, for example, Zigbee, Bluetooth, Wi-Fi, WiMAX, LoRA, HART, and so forth are current wireless WAN frameworks. However, shaping a satisfactory and enthralling IoT framework appears to be an arduous test, due to various network compositions. One of the most important issue is information privacy and network protection. However, due to the tremendous advances in technology, efficient energy and data management systems are making IoT systems productive [1].

Currently, IoT applications are driving medical care in a significant way; additionally, inventions of various WSN medical devices (from elderly care to health monitoring in remote areas including health database and serious disease) are emerging as blessings of science. The pith of the Internet of Things constitutes various network protocols, which operate various wireless medical sensors and imaging devices. During the COVID-19 pandemic, IoT played a significant role in the healthcare sector. People received treatment from home through telemedicine

---

T. D. Mou

Department of EECE, Military Institute of Science and Technology, Dhaka, Bangladesh, India

G. Srivastava (✉)

Department of Math and Computer Science, Brandon, Canada

e-mail: [srivastavag@brandonu.ca](mailto:srivastavag@brandonu.ca)

and get prompt consultancy for various health issues by connecting to physicians through various IoT devices; meanwhile, many people were protected from coronavirus infections by obtaining the latest information about the coronavirus-infected area [3].

This chapter highlighted the IoT architecture, network protocol, and security requirements of the healthcare sector. Focusing on data transfer protection, we have discussed the future aspects of establishing network protocols of IoT in the medical sector. The foremost feature of this chapter is to systematically demonstrate the internal schemes and mechanisms of the IPv6-constrained network protocol through the study of different surveys and tutorial work. In addition, we have described the existing network protocols associated with IoT in healthcare and some constantly updated network solutions. Due to the sensitivity of the information in the healthcare sector, network protocols get precedence before they can be applied to the system. At last, focusing on future challenges, the patterns of IoT domain hosting devices have been examined explicitly.

## 2 Overview of Network Protocol

Fire lights, smoke signals, or drums were the primary forms of telecommunication. The main drawback to these communication frameworks is that these transmit a set of predefined messages. The International Telecommunication Union (ITU) states that the transmission and reception of encoded data as signals via electromagnetic systems is telecommunication. The US Department of Defense (DoD) built an organization to launch the Internet called ARPANET (Advanced Research Projects Agency Network). It consists of four hubs investigated at the College of California, Los Angeles, College of California at Santa Barbara, and College of Utah. On 29 October 1969, UCLA and SRI traded the primary message; in 1972, Roy Tomlinson sent an email to Jolt Beranek and Newman, Inc. (BBN) after UCLA had been associated with BBN.

A network protocol is a set of verified systems that facilitate instruction on how to arrange, broadcast, and receive data so that computer network devices (from servers and routers to endpoints) can communicate despite the differences in their fundamental foundations, plans, or principles. In essence, it permits linking gadgets to communicate through each other, despite several differences in their internal processes, construction, or design. Moreover, the network protocol is playing a modern role in digital communication. Moreover, the devices are interconnected in the sense that the predefined regulations in the software and hardware of the device appear together. Local area networks (LAN) or wide area networks (WAN) are powered by network protocols.

## 2.1 List of Network Protocols

Almost thousands of network protocols have been intuited, due to advancements in network technology; however, all of them compile into three primary divisions [4]:

- I. Way of communication
- II. Network management system
- III. Security

For the smooth operation of network devices, each type is essential, and they must work together to facilitate that usage.

### 2.1.1 Communication

Different network devices follow communication protocols to liaise with one another. Analog and digital communication systems will accomplish maximum connectivity for transferring various files from the device and web access.

The following systems are commonly used for communication protocols:

- *Automation*: Automated systems depend on an automation protocol, which is used in every business and private sector for the advanced building development, cloud technology, or self-driving vehicles.
- *Instant Messaging*: WebSocket and XMPP are two main protocols for instant messaging for text-based communications on WSN devices.
- *Routing*: The communication between the routers and other devices on the network follow routing protocols. Ad hoc networks are specifically associated with routing protocols.
- *Bluetooth*: A variety of Bluetooth protocols work on classic Bluetooth devices, such as headsets, smartphones, and computation work.
- *File Transfer*: File transfer protocol (FTP) controls moving files while transferring files from one device to another device through physical or digital medium.
- *Internet Protocol*: Data can be transported across networks and attain the right destination by following a set of routing and addressing packets of data.

### 2.1.2 Network Management

Network management protocols govern how effectively a computer network operates the various procedures needed to perform. Various types of devices on a single network could be affected by these protocols, for instance, the connection between computers, routers, and servers ensures that in the entire network, they individually perform optimally. Network management protocols consist the following operations:



- *Connection*: Devices follow the network management protocol to establish and maintain steady associates between altered devices on the same network.
- *Link aggregation*: Two devices will connect into a single link by combining several network connections. Additionally, if one of the links becomes damage, nevertheless, remains a strong connection and maintains the sustainability of that connection.
- *Troubleshooting*: Network administrators investigate network connections in detail to identify errors that reduce network performance and find ways for administrators to troubleshoot.

### 2.1.3 Security Protocols

Security protocol, also known as a cryptographic protocol, works to ensure the arrangement of information and protect the transmitted data through its unit area from unauthorized devices.

Some common functions of security network protocols are as follows:

- *Entity Authentication*: This protocol creates a framework for accessing protected areas that sometimes require individual gadgets on a system to ensure their features.
- *Transmission*: It is better to use transportation security protocols to ensure information when transmitting from one network gadget to another.
- *Encryption*: The system requires encryption protocols to input any secret keys or passwords to allow the user to access that data to secure information and protected areas.

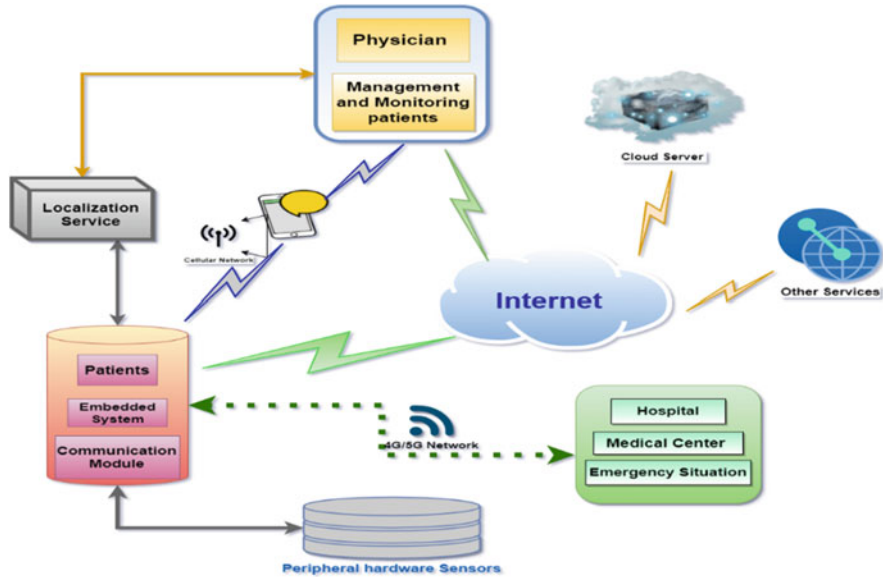
## 3 Network Protocols for IoT

The following era is defined by IoT – the sector of innovation that is bringing gigantic changes in the industry, pharmaceutical, natural care, and urban improvement. Lots of obstacles must be considered when shaping this vision, for instance, evolving interoperability issues, security, data encryption requirements, and the updated base of proficient administration frameworks. Accessible IoT communications focus on the importance of routing conventions and developing IoT applications. An intensive layer-based convention scientific categorization is mentioned below, along with an explanation of how organized conventions fit and work to address future IoT necessities and applications.

- *Categorization IoT Protocols*: Instead of compiling the entire IoT Protocols into a significant design model such as the OSI model, protocols can be divided into different levels. These are mentioned below (Table 1).

**Table 1** Categorization IoT protocols

Framework	RPL, IPv4/IPv6, 6LowPAN
Recognition	URIs, IPv6, UCode, EPC
Transmission	LPWAN, Wi-Fi, Bluetooth
Origination	mDNS, Physical Web, DNS-SD
Data protocols	MQTT, CoAP, AMQP, WebSocket, Node
Organizing device	OMA-DM, TR-069
Multilayer frameworks	HomeKit, Weave, IoTivity, AllJoyn



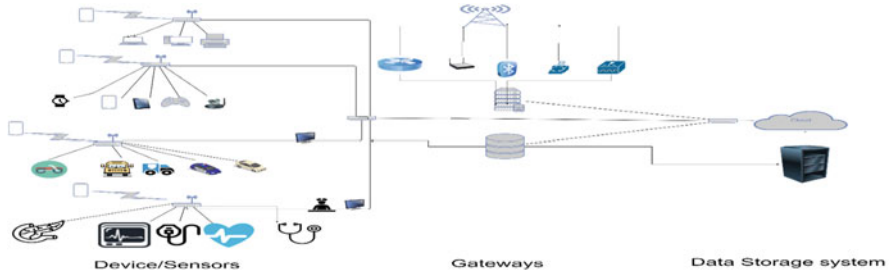
**Fig. 1** IoT healthcare system architecture [5]

### 3.1 IoT Healthcare Networks

The IoT healthcare application includes an ECG waveform with monitoring the human body’s heart rate, blood oxygen, body temperature, etc. [5]. Specialists and patients can understand record capacity through helpful media, vast demonstrative capabilities without specific training on utilizing IoT healthcare applications, and the meaning of signs (Fig. 1). Sequentially, the recorded data notice the personal profiles of individual patients for future reference.

This IoT stage has full access to establish communication remotely, which permits the application to form and arrange attachments to utilize, custom, and organize conventions.

WBS sends information to the Android interface through Zigbee, Wi-Fi, Bluetooth, or Ethernet. Thus, the Internet or cellular system requires authorization to



**Fig. 2** IoT system architecture [5]

receive the information. The form of gadgets recognizes communication systems and associations. WSN permits the application to arrange and find the nearby devices.

### 3.1.1 Classification of IoT Healthcare Connections

The IoT system has three-level architecture:

- I. Devices
- II. Gateways
- III. Data systems and analysis (Fig. 2)

- *Device to Device*: Coordinate contact between two close objects when they share data immediately without the middle platform. For example, mechanical robots and sensors are associated with one another straightforwardly to arrange their activities and perform assembly of components proficiently. This sort of association is uncommon, though most gadgets are unable to handle such forms.
- *Gadget to Gateway*: Broadcast communications between sensors and portal hubs. Doors are more capable of computing gadgets than sensors. They have two fundamental capacities: (1) to solidify information from sensors and course it to the comprehensive information framework and (2) to analyze information upon finding issues and return it to the gadget. Different IoT portal conventions will be better suited to this arrangement, depending on the portal computing capabilities, capacity arrangements and unwavering quality, recurrence of the information era, and its quality.
- *Gateway to Information Frameworks*: Information transmission from a gateway to the fitting information framework. To decide what protocol to utilize, the user should analyze information activity (recurrence of business and blockage, security necessities, and how numerous parallel associations are needed) between information frameworks and data exchange inside information centers or clouds. Conventions for this type of association should be simple to convey and coordinate with existing apps and have high accessibility, capacity, and solid catastrophe recuperation.

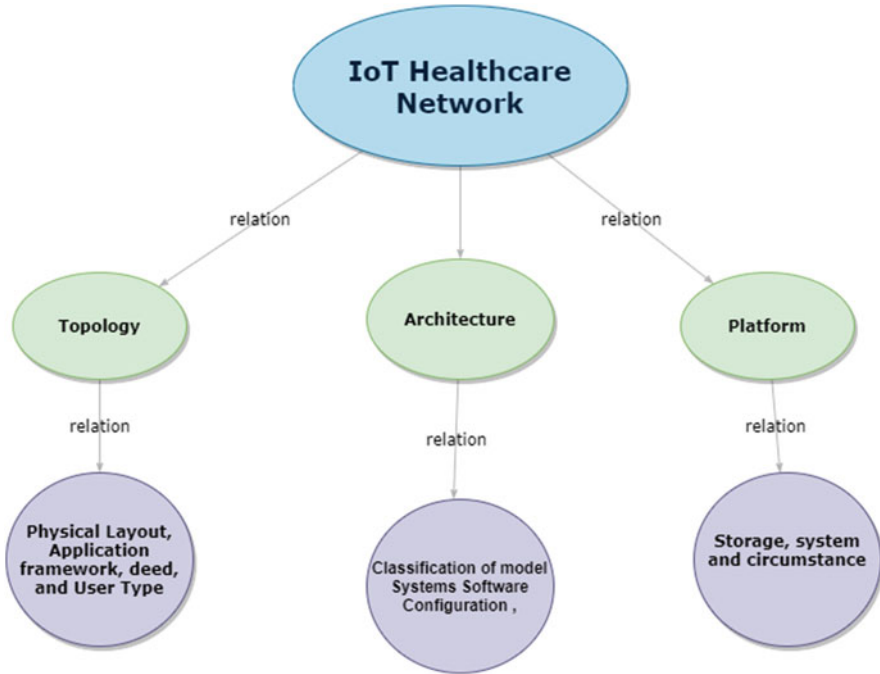


Fig. 3 The IoT healthcare network topology [6]

The IoT healthcare network performs an essential role in medical technology. Medical data is accessed easily for transmitting and utilizing healthcare-tailored communications, as well as the advantages of IoT can be acquired from the IoT healthcare network. Figure 3 represents the IoT medical network structure [7].

### 3.1.2 IoT Healthcare Network Topology

The network topology of IoT healthcare establishes the activity of various components of its organization and creates an agent status to display the coherent healthcare situation. The featured aspects of IoT healthcare networks are to support the IoT base, encourage the transmission and mobilization of therapeutic information, and strengthen the utilization of communication mediums in line with healthcare.

As shown in Fig. 3, this segment examines the IoT healthcare network topology, engineering, and stage. In any case, it states proposed models are treated as a great starting point for incorporating experiences into the IoT arrangement [12] [67].

A heterogeneous computing network is responsible for collecting multiple sensor data like body temperature, oxygen saturation, electrocardiograms (ECG), etc. The conceptual graph of IoT-based healthcare systems for detecting an object

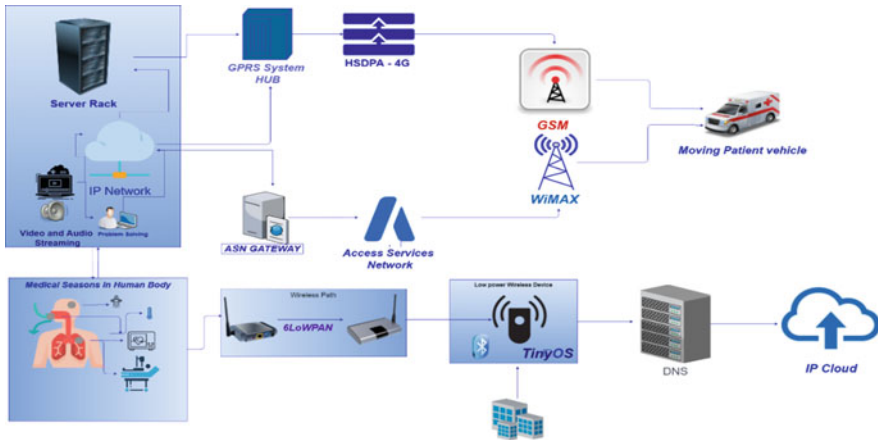


Fig. 4 IoT healthcare network topology appearing in the role of a portal

in real-time is commonly known as the IoT healthcare network topology. IoT converts tablets, smartphones, versatile electronic gadgets and recovery terminals into shifting numerating networks [6].

The topology in Fig. 4 illustrates the recording of magnetic resonance images using a simple network microwave WiMAX combination of comparative conceptual structures. The combination of Internet protocol (IP), GSM, standard gateway and the benefit of systems is Comparative Conceptual Structure. Figure 4 also imagines a situation where a patient’s health profile and vitals are captured by the body using convenient therapeutic gadgets and sensors. Right off, different sensors analyze and save captured information, resulting in machines becoming valuable for conglomeration. Clinicians can monitor patients from any region and respond appropriately based on the history of the investigation and collection of data records. Topology incorporates a required organized structure for supporting the spilling of therapeutic recordings. Embedded component-based operating system TinyOS serves low-power wireless devices and platforms as an open-source BSD-licensed.

Figure 5 represents the IoT healthcare network topology portal, where pharmaceutical packaging (iMedpack) demonstrates an IoT gadget that intelligently manipulates drug abuse. The wearable sensors of IoT devices send information to the IoT cloud of the healthcare network through the healthcare gateway, which increases the potentiality of detecting diseases and suggests other diagnoses.

The portal itself can explore, store, and show all collected information [7]. The authors of [8] explained a similar IoT healthcare network topology, which combines classical gadgets with the IoT healthcare initiative base. At the same time, distinguishing related exercises and parts in therapeutic administrations could be essential in planning the IoT healthcare network topology, as shown in Fig. 5.

Healthcare benefit providers claimed pre and post-treatment preparation, including healthcare administrations. The framework of crisis curative administrations

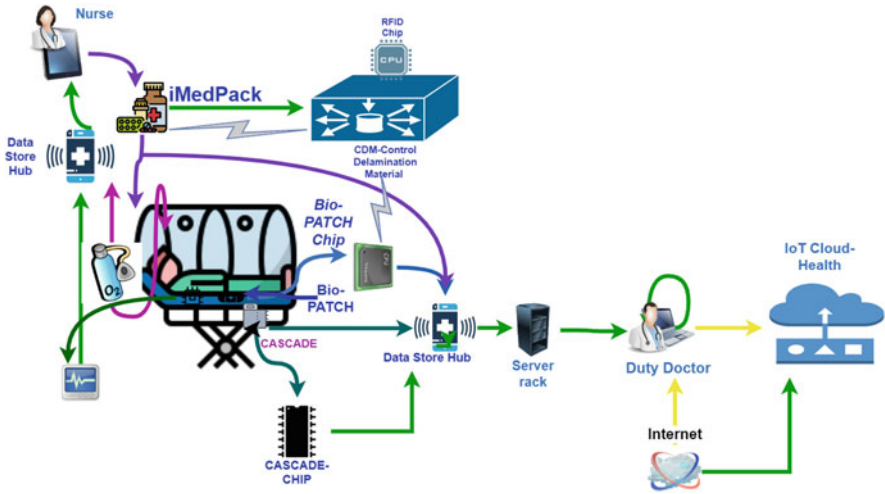


Fig. 5 IoT healthcare network topology in healthcare portal

illustrated such healthcare exercises [9]. Moreover, cloud computing is associated with IoT healthcare network topology for inescapable well-being concerns [10], which run as an ordinary complete mesh networking system in the pervasive Internet. In this circumstance, the topology must incorporate a therapeutic run to show a framework within the case of a semantic restorative observing framework [11].

### 3.1.3 IoT Healthcare Network Architecture

The physical components of the IoT medical care system and their supported system and strategies of working standards determine the provided layout of the IoT healthcare network. Figure 6 depicts the telemedicine with all-encompassing assisted active frameworks prescribed by the Continua Health Alliance. The IoT portal interfaces connected to the distant neighborhood use a wireless local area network (WLAN) for assuring that the IoT gateway and caregivers have secured communications [12]. A general-purpose sensor network designed to operate independently through a variety of therapeutic sensors and machines is called the wireless body area network (WBAN).

Figure 6 depicts the 6LoWPAN layer structure. Moreover, IPv6 and 6LoWPAN frameworks work for transmitting information over the 802.15.4 convention by using the IoT healthcare network concept and wearable sensors. After that, the user datagram protocol (UDP) helps to return the information at the sensor hubs [15]. A subset of portable IPv6 (MIPV6) and IPv6 convention portability is unsupportable with 6LoWPAN. This is the limitation of 6LoWPAN (Fig. 7).

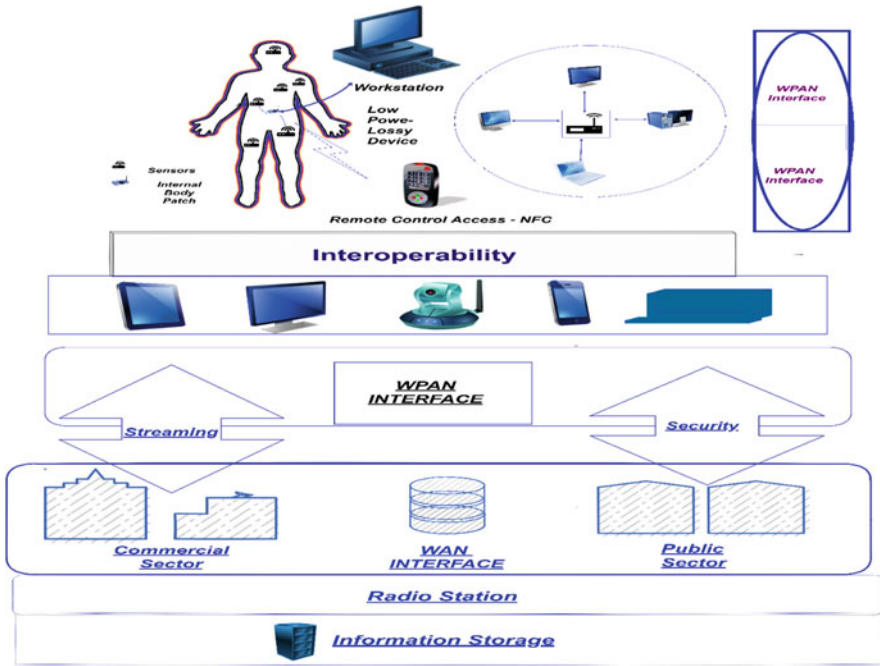


Fig. 6 The IoT healthcare network architecture

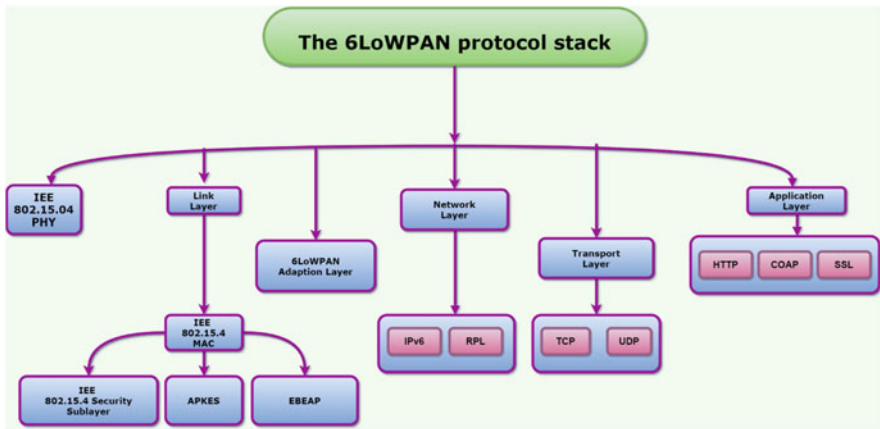


Fig. 7 Continua Health Alliance

In [13], the authors mentioned that the 6LoWPAN portability arrangement is a convention of trading messages between multipurpose understanding centers, base systems, and moving systems. The following are four elective methods considered in [16] to address portability:

- I. Requesting switches count
- II. Holding up for an unused coordinated non-cyclic chart (DAG) data protest (DIO)
- III. Joining other accessible origin hubs
- IV. DAG data requesting (DIS) message transfer

Among these, requesting switches and sending DIS messages to communicate is one of the quickest strategies due to self-starting versatile hub nature. The convention stack is demonstrated by [17] as a common portal for community recovery administration. Also, for community restorative administrations, the normal portal convention stack is depicted by [17]. This stack clearly illustrates how the HetNet monitors incidental activity, abnormal activity, and query-driven activity. A complex e-health benefit convenience strategy is proposed [17] based on three steps: computation, signaling, and data transmission calculations. Signaling serves as an asset-determining mechanism between complex benefit composition, quality-of-service (QoS) transactions, and IoT healthcare networks.

Vehicular systems also accommodate medical gadgets for capturing real-time information regarding patient health through the server application of IPv6. The light auto-configuration conference, shown in Fig. 8, presents the vehicle-to-infrastructure (V-I) communication within the IoT healthcare network. Thus, the IPv6 course employs a default sequence of directing tables.

It provides a set of IPv6 addresses for gadgets in a vehicle. The degree of information structure in healthcare administrations and the address of different communication benchmarks facilitate the rise of the IoT healthcare network [19, 20] due to reshaping information. Information supply engineering gets evaluated in the case of cloud computing integration [9]. This structure of the IoT healthcare network platform has been described in the following paragraphs, which contains both design and medium.

### 3.1.4 Networking Platform: IoT Healthcare

The IoT healthcare network stage mentioned the systematized platform and calculating stage simultaneously. Figure 9 [21] represents a benefit stage system centering on residents' health information. This system systematically displays multilayers so that with the help of back-level suggestions, agents can get to different databases from the application level.

Interoperability regularity across collaborators of the IoT healthcare network is approaching as the purpose of an extensive stand, which is the significance of standardizing [10]. The interfaces of computing tools and programs, the fitness information group (e-health record, digital version of the patient's paper chart), and the security plan are the three sections of interface standardization for setting up a unified scheme. It will inevitably ensure associated interoperability. Reference [11] contains the proposal of a comprehensive view of the administration, monitoring, and diagnostics stage of the IoT healthcare network, particularly for recovery. As



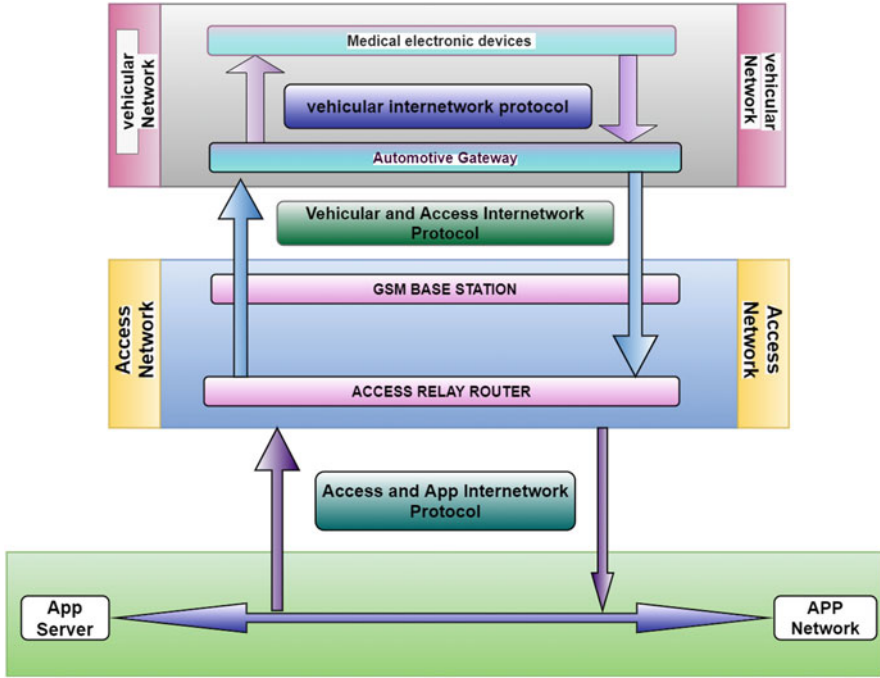


Fig. 8 Vehicle-to-infrastructure (V2I) communications within the IoT healthcare network

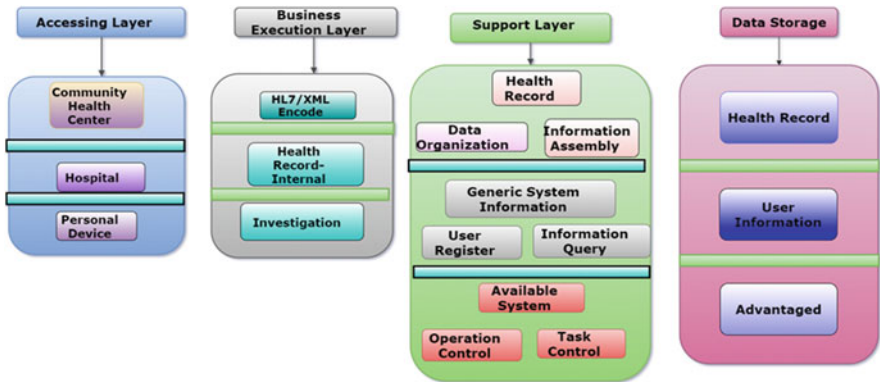


Fig. 9 Health information service model functional framework

shown in Fig. 9, this planning system incorporates the user interface, interdisciplinary progress, and reinforcement (Fig. 10).

An event-driven middleware bundle called VRTUS made the function easier to investigate and compress IoT healthcare applications. Based on XMPP, adaptive communications get received through the IoT healthcare network, which results in

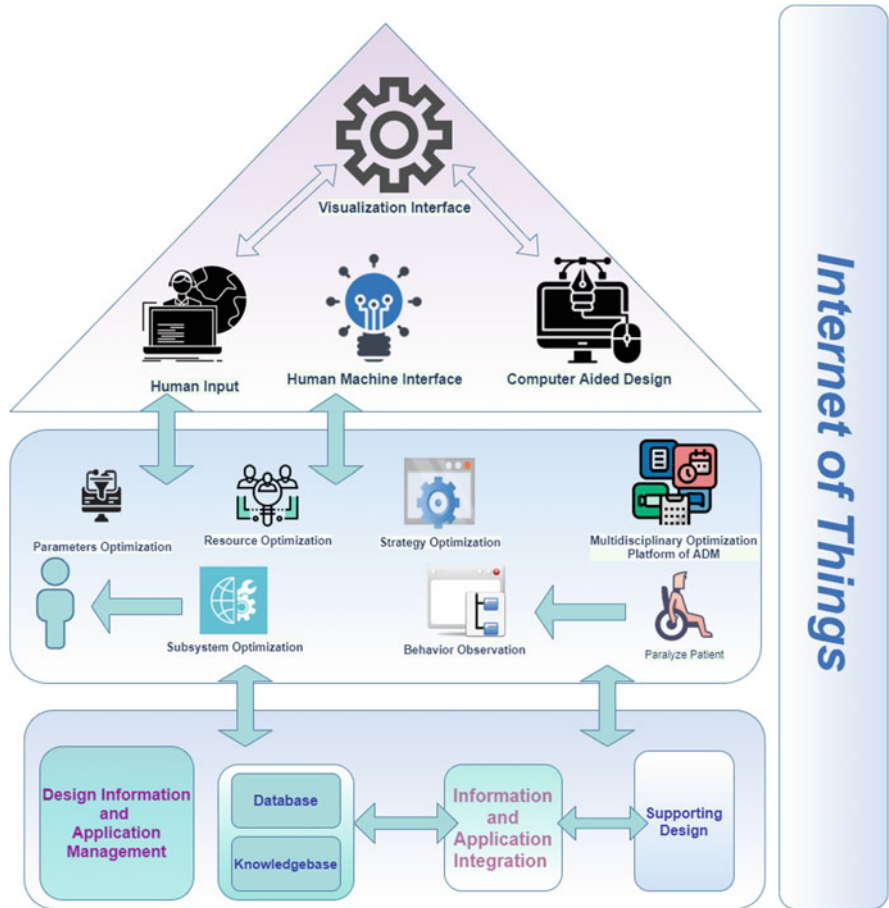


Fig. 10 A framework of an automation design methodology

a conference-aware network. Article [12] contains the proposal of a strategic IoT structure that strengthens the portal, ensuring the management of ample clients with different sensors. This strategy provides an algorithmic view of the gateway that separates unclaimed welfare information from the end switch and personalizes the captured data in the database into predefined data. IoT has created a three-tier cloud platform for accessing ubiquitous cloud information through the healthcare network [9].

The occupant database layer stores multitenant databases. The asset level is reliable for controlling the receipt of information and for sharing information with interconnection. The trading level performs the necessary adjustments. Resource Control Management situations and Home Automation gadgets supply information with some denotative capabilities. Semantic layers of these devices support four sorts of ontologies.

## 4 Connecting Protocol of IoT

### 4.1 Message Queuing Telemetry Transport (MQTT)

MQTT defines as a basic way of providing resource-constrained operations among clients to disseminate telemetry data by using machine-to-machine (M2M) communication over a thin informing protocol, where the IoT protocol use in publishing/subscribing communication design. Figure 11 demonstrates an MQTT structure. MQTT convention may be a beneficial remote arrangement, and it will encounter different sorts of delays due to incidental transmission capacity restrictions or questionable connections.

The MQTT convention encompasses a client and a broking. An MQTT broking could be a server, as the clients are the associated contraptions. When an apparatus or client wants to send data to a server or merchant, it is called the publisher. The relationship from a subscribing supporter to a broking breaks at a point when the

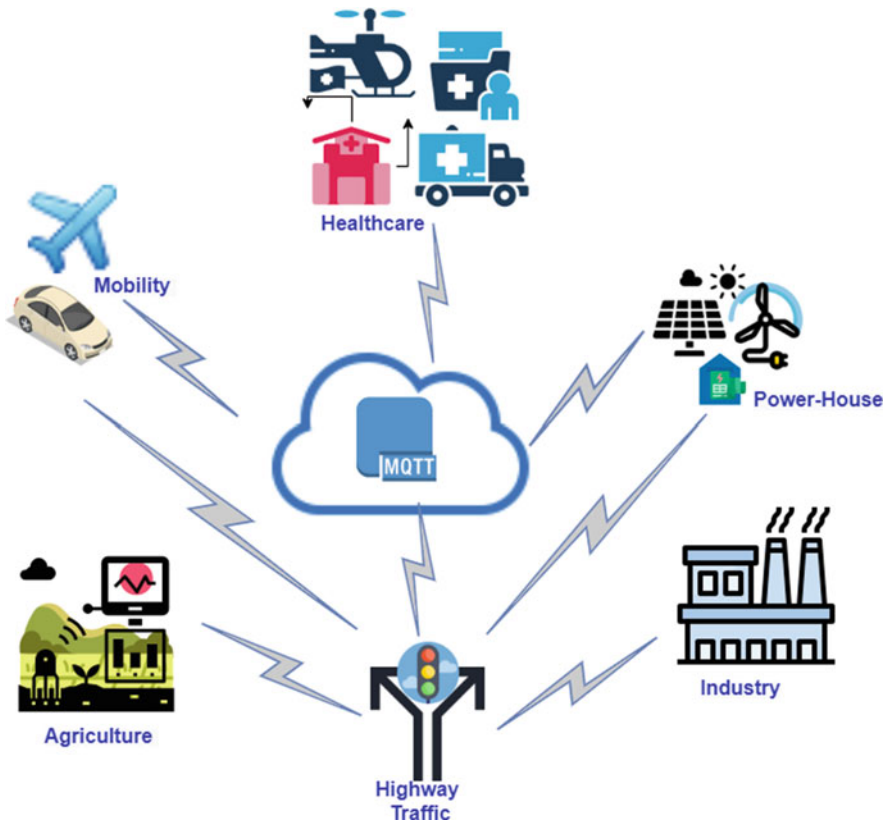


Fig. 11 Message Queuing Telemetry Transport (MQTT) structure

merchant will buffer messages and thrust them out to the endorser while it returns online. In this circumstance, an association from the distributing customer to the merchant gets disengaged without any observation. Then, the merchant can close the relationship and send endorser a cached message with information from the publisher.

MQTT permits resource-restricted IoT gadgets to send or submit approximate statistics of a given topic to a server, which functioned as an MQTT message broker. Brokers overcome previously subscribed subjects who hand over statistics to those clients. To humans, a topic seems like a classification document course. A selected stage of a subject' hierarchy uses a wild-card specification for subscribing to multiple tiers by customers.

#### **4.1.1 MQTT: Quality of Service (QoS)**

It is the contact between the sender and receiver to receive data accurately. Among the three levels of service of MQTT, the client avails the opportunity to select any service. Among these, the first one is safer for high bandwidth and more latency.

Unacknowledged service is one of the most straightforward QoS operations. PUBLISH packet sequence is used in this service, wherein the publisher sends a message to the brokers in real time, while the brokers provide that message to the subscribers.

The second stage is an acknowledged service that uses the PUBLISH/PUBACK packet sequence in the middle of publisher-broker, broker-subscriber for real-time data transfer by verifying the message received accurately. Moreover, reconstruct the system to resend the original information if the acknowledgment is not accepted by the receiver promptly, which contains two pairs of packets. The third plane of QoS is Assured Service or QoS2, that's a pair of PUBLISH/PUBREC, and another one is PUB REL/PUBCOMP. The significant function of these functions is to confirm data delivery once without the regeneration of the message.

#### **4.1.2 MQTT Applications**

Currently, some social media applications are using MQTT protocol to consume battery power in devices. MQTT is very reliable in real-time computation for M2M and IoT devices, such as controlling and maintaining environments in different industries like healthcare, manufacturing, automotive, etc. The MQTT protocol potentially facilitates the healthcare system by consuming less power and bandwidth.

#### **4.1.3 Benefits of MQTT**

- Concise data packets utilizing a low network.

- Effective data distribution.
- Wireless gadgets can operate on a low network.
- Efficient for the attached devices for adopting low power.
- Reduce bandwidth, as well as fast and guaranteed data delivery.

#### 4.1.4 MQTT Limitations

In comparison to CoAP, MQTT obtains a slower transmit cycle. In terms of security, it was unimplemented on privacy concerns, and it is also unencrypted, but it does use TLS/SSL for secure encryption. On the other hand, due to binary message payloads, there is a lack of interoperability. The authentication process is not simple; there is no observation of data transmission between end-to-end devices. Hence, any harmful information can interrupt either intentionally or by mistake.

#### 4.1.5 Current Aspects of MQTT

MQTT was authorized officially as one OASIS standard [68] on October 28, 2015. Later, at the early stage of 2016, it was granted as a standard of International Standardization Organization (ISO). At present, MQTT has collaborated with WebSocket, which is a two-way communication protocol between client and broker. Later on, the v3.1.1 standard and the v5.0 standard became included in the updated version of MQTT and approved as OASIS standards.

## 5 Network Encapsulation Protocols for IoT

### 5.1 6LoWPAN

6LoWPAN is an IP-based technology (IPv6 low-power wireless personal area network) under IEEE802.15.4 standard and operates solely within the pair of 2.4 GHz frequency in 250 kbps transfer rate variation. Therefore, the latest Network Protocols for the Internet of Health Things competition for Zigbee with 6LoWPAN allow the tiniest devices through restricted processability to transmit info wirelessly, exploiting web protocol. Therefore, the latest contest between Zigbee and 6LoWPAN is to allow the smallest devices with limited processing to send data wirelessly using any web protocol.

One of the foremost imperative plans in the IoT sector is the 6LoWPAN convention. An irregular header squeezing and a reduction in over-transmission characterized the 6LoWPAN protocol, where most of the 128-byte IEEE 802.15.4 standard outlined involves displacement handle capacity to cover the obstruction. Subsequently, IPv6 defines the entire 1280 bytes [4], and 127 bytes 802.15.4 MTU

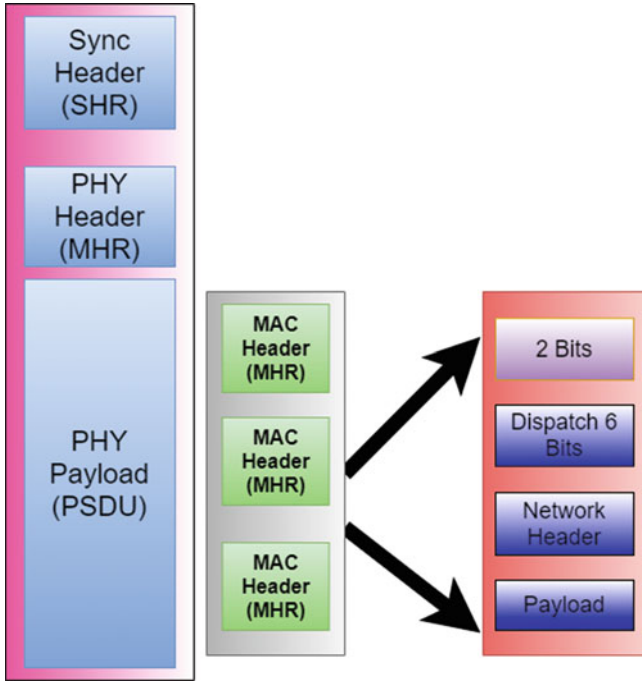


Fig. 12 6LoWPAN packet

divides the minimum IPv6 of a Maximum Transmission Unit (MTU) is being divided [38].

The dispatch header (LOWPAN\_IPHC header) determines the types of packets by taking six bits once (dispatch field). The remaining structure alternates with the filtered segment. 6LoWPAN holder defined actualized specific style supported. Four types of headers, i.e., 6LoWPAN (00), dispatch (01), mesh (10), and fragmentation (11), are excluded from the structure. Frames that are not consistent with the 6LoWPAN parameter will increase when the 6LoWPAN header is missing. Sending title through IPv6 is used for title shortening and multicasting (Fig. 12).

Victimization fragmentation headers are enabled for 128-byte fragmented dissonant large IPv6 headers, whereas mesh headers support broadcasting.

Besides, 6LoWPAN adopts conventional routing schemes to provide efficiency between existing IP devices and low-power devices [22]. A large organization of IP-based administration, processes, communications equipment, and assistance benefits from 6LoWPAN.

Devices contain a substantial amount of IEEE 802.15.4 link-level processes for security issues. IEEE 802.15.4 authentication and encryption require 128-bit advanced cryptography prediction. Furthermore, end-to-end security allows a mode of encapsulating security payload (ESP) that uses advanced encryption using

cipher blockchain message authentication codes (ES-CCM) or standard counter with IPSAC traditional terminal.

## 5.2 *6TiSCH*

The IEEE 802.15.4e pattern includes time-slotted channel hopping (TSCH) and low-power and lossy networks for designing several wireless ultralow-power networking embedded devices [25–27], as shown in Fig. 14.

The unicast or broadcast communication at the medium access control (MAC level) on the TSCH network is distributed in the autonomous protocol cell and split time. The outlines of the various beginnings indicate a pattern that repeats constantly. The following three options support an agenda to pick each node in each slot: (a) transfer, (b) receive, and (c) rest. Time slot operation saves energy by reducing conflicts and allows the use of various arrangements.

### 5.2.1 *6TiSCH Protocol Stack*

Logical link management (LLC) is a part of the 6TiSCH operation sublayer (6top) [15], which uses the TSCH MAC layer to extract and process the accompanying facts of hyperlinks, control the TSCH schedule, collect attribute data, and monitor the performance of the video display unit link (cell). Channel allocation control scheduling using a matrix that consists of accessible time slots, in which network scheduling tasks are plotted in rows and exchange frequencies are plotted in columns. Any networked devices are accustomed to the resources of this matrix.

A concise format of the IPv6 routing protocol (RPL) is located in IPv6 bundles through a routing header of 6LoWPAN (6LoRH) [28], whereas the header compression of 6LoWPAN compressed UDP and IPv6 headers [29]. The four ways of managing schedules are combined with three utterly complex forwarding models [22]. The entire regulation of CoAP management interface (COMI) executes from 6TiSCH, which carries datagram transport layer security (DTLS) protocol. The system architecture develops link-level protection by enabling modification to the counter in the shortest time between connected devices and enabling CBC-MAC protection.

## 5.3 *Zigbee IP*

The Zigbee scientific branch is defined as the initial open common protocol that manages cheap and low-cost devices through IPV-based complete wireless mesh networking to provide uninterrupted web property. Fundamentally, the collaboration of the IEEE 2030.5 standard with Zigbee's scientific discipline was referred to as

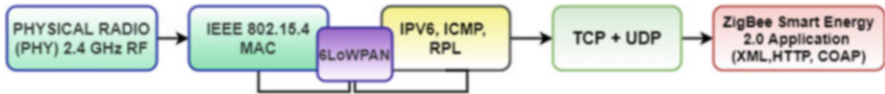


Fig. 13 Zigbee IP scientific discipline stack



Fig. 14 6TiSCH protocol stack [30]

Zigbee’s good energy era [23]. Based on the low-level use of the IEEE 802.15.4 standard, the Zigbee scientific discipline stack is shown in Fig. 13. To reduce the burden of communication and increase the capacity of the network, the title shortening method of 6LoWPAN has been used (Fig. 14).

Each network node must be auto-addressed using routing protocols with IPv6 addressing. Routing protocols and IPv6 automatically address a specific network node. Zigbee scientific discipline allows Zigbee End Device (ZED) and Zigbee Router (ZR) to control the Zigbee Coordinator (ZC) tool by combining multiple networks. The controlling and network foundation is connected with the Zigbee Coordinator. When necessary, ZEDs receive information from ZRs to rescale the network [24].

An extensible authentication protocol (EAP) is a protocol for carrying authentication for network access (PANA) because it allows interface authentication between the consumers and the access network by accepting the network Layer. Furthermore, the PANA convention managed both transport security layer (TLS) 1.2 and elliptical curve cryptography to support the manipulation of application privacy to manage network access. Based on the 602.15.4 pattern, another end of the Zigbee scientific discipline occupies the obscure truth that it provides the last IPV property of the expandable design victim. Therefore, IoT applications serve as a committed investment in the Zigbee scientific division.

### 5.4 6Lo-IPv6 (6Lo) Working Group

Different data links are transmitted through the IPv6 transmission frames by following updated rules of conducting the 6Lo-IPv6 (6Lo) working group on the resource-constrained network node in the IETF [30].

Multidisciplinary/multicast/broadcasting characterized resources hubs, such as preparation, memory and control resources, state-of-the-art limitations, cycle with code space management, transfer speed including vitality optimization, and entire





**Fig. 15** IP over G.9959 convention stack

gadget network. Firstly, the IEEE 802.15.4 and IEEE 802.15.4e standards protect the 6LoWPAN and 6TiSCH working group; then, the data link binds the 6Lo working group. Moreover, Request for Comments (RFC) also includes some of these 6LOs.

## 5.5 IPv6

IPv6 is the updated version of the Internet protocol, which is a distinguishing proof and a framework for computer systems and field activity over the Internet across multiple IP networks. Moreover, Internet layer protocol IPv6 is widely extended and utilized for packet-switched internetworking and provides end-to-end datagram transmission. Furthermore, the IPv6 address occupied 128 bits. The space plane is the logic of a distinct plan for comparing the IPv4 over the IPv6 address, which subletting was utilized to progress the effectiveness of the utilization of the concise address space.

### 5.5.1 IPv6 over G.9959

The short-range thin-band advanced radio handsets fix configuration formation for conducting IPv6 data units in ITU-T G.9959 systems through RFC 7428 [22]. IPv6 packets over the ITU-T G.9959 network layer are shown in Fig. 15. Multiple segments establish the G.9959 system for equitable factor, which generates a combination of different hubs.

The domains contain nine separate systems, which suggest that the hub collection is achieved by similar means. A solitary 32-bit HomeID image identifies specific space with 232 hubs (Space S count) [31]. G.9959 HomeID compares to an IPv6 subnet for utilizing or representing a part of IPv6. Rather than a 16-bit brief address, each hub in the selected domain is associated with an 8-bit NodeID identifier. First, a G.9959 interface-level address creates a relational interface image for establishing a link-level IPv6 address, and then the ability to compress into the G.9959 profile is obtained. IEEE 802.15.4-based system used header compression arrange to fix one of the connected addresses. Apart from this, segmentation and reassembly (SAR) is used when the G.9959 media control the convention information unit (MAC PDU), where the G.9959 is smaller than the layer for transmitting packets. A common network key, like RFC 7428, is used to provide a level of security for cryptography.

However, for strict security demands, it uses its high-level security projects for the foremost awareness in verification and peer-to-peer encryption. The location of the ITU-G.9999 Z-Wave representative protocol can also be predictable.



Fig. 16 The Bluetooth LE stack

### 5.5.2 IPv6 over Bluetooth Low Energy

The use of the 6LoWPAN specification model for IPv6 transportation through the connections of Bluetooth low power (LE) is defined as RFC 7668 [32]. The Bluetooth LE stack of the IPv6 and protocol assistant carrier (IPSS) is depicted in Fig. 16. There are three protocols to maintain a popular protocol stack and to collect the standard’s convention stack [22]: the logical link control and adaptation protocol (L2CAP) for the upper layer, the Generic Attribute Profile (GATT), and the attribute protocol (ATT).

GATT is used in every Bluetooth device, including clients, a server, and other types of devices. The lower layers cover with the host controller interface (HCI); however, the multiplexing record of the upper layer creates some fault in the L2CAP sublayer, as well as long data packets being divided and reassembled for its license.

Peripheral and critical devices *connect* with direct Wi-Fi in Bluetooth LE. A device in a valuable role can handle individual parallel connections with numerous surface gadgets. A single principal may drive a peripheral device but can also work on multiple devices at the same time. Two peripheral devices are capable of working together by adopting the service of IP routing, which is aligned with the respective specification.

The main reason for the protocol overhead dimension restriction in the Bluetooth LE unit is to consume low electricity. Since gadgets are split and reused into 27-byte L2CAP data packets through the L2CAP sublayer, the required separation technology does not include 6LoWPAN. One of the significant drawbacks is that a multi-hop hyperlink layer network can not be established in the Bluetooth LE module. Alternatively, low-power peripheral gadgets get the statistics from an important node origin. Therefore, peripheral and bulk gadgets will gradually operate 6 6LoWPAN border routers (6 LBR) and 6 6LoWPAN nodes (6LN). Nevertheless, the required field obtainment occurs through IP routing capability, based on the related specifications of exchanging internal peripheral information.

The collaboration of IPSS with the Internet Protocol Support Profile (IPSP) permits the established link-layer connectivity and IPv6 protocol for delivering IPv6 datagrams, which support decision devices. In terms of security considerations, the CBC-MAC (CCM) strategy and an ES block cipher merge with Bluetooth LE counter for providing authentication and encryption at the link level. Only higher-level layers can avail of this feature [33].

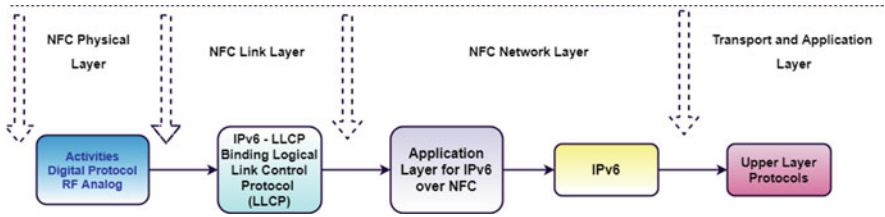


Fig. 17 Protocol stack for IPv6 over NFC

### 5.5.3 IPv6 over NFC

A connection between two electronic devices generates from near-field communication (NFC), where the initiator generates a radio frequency field and can reinforce a passive target between the common device and target device. The RFID system efficiency has improved through NFC by allowing two-way communication between gadgets. Figure 17 [34] represents the protocol stack for IPv6 over NFC. Higher layers occupied with delivery protocols (UDP and TCP), application protocols, and other protocols can protectively run over IPv6.

#### IPv6 over NFC Protocol Stack

Fundamentally, the logical link control protocol (LLCP) monitors MAC multiplexing mechanisms. Besides, LLCP provides LLC, which contains three components: hyperlink control, wireless delivery, and connection-based transport. Multiplexing strategies integrated existing Wi-Fi protocols into LLCP formats. NFC-enabled peer devices' LFCP protocol data unit (PDU) introduced an IPv6 datagram that roamed below NFC's LLCP for connecting information to the NFC in IPv6. A sort of logical link manages the DSAP (the destination NFC-enabled tool dealing with LLC) value of the IPv6 over NFC protocol, represented by a 6-bit identity of the LLCP entry point (SSAP) by transferring the source carrier. Certain transmissions of IPv6 packets can be adjusted because of the limited RF distance, though scanning may mitigate vulnerability exploitation and place tracking.

### 5.5.4 IPv6 over MS/TP (6LoBAC)

RS-4355 single curved pair PHY [22] master-slave/token-passing (MS/TP)-based protocol defines in BSNET as a widely used statistical link protocol. Alternatively, which considered as the emphasis of IEEE 802.15.4 standard for conducting a competition-free MAC layer. MS/TP-based devices generally include low-memory, low-power electricity, and a low-cost microcontroller.

MS/TP also contains a program named universal asynchronous receiver-transmitter, which is the combination of UART, an RS-485 transceiver, and a 5 ms decision timer. The multipoint bus allows MS/TP to enter through a token. The nearest node storing token of MS/TP token can initiate an unrequested record switch most efficiently. The following group node (constant with its MAC address) accepts the token; after that, the new graph node transmits the predefined maximum range token toward the recording device. 6LoWPAN is less particular than MS/TP for at least three factors:

- Fake routing or hidden nodes are unable to create a problem due to a direct connection between All MS/TP devices.
- The maximum cutting-edge.
- The MS/TP specification can help to extend the payload, eliminate segmentation requirements, and reorganize below IPv6.

Other than this, 6LoBAC is an innovative outline for IPv6 embodiment that incorporates a header compression component and progresses MS/TP connect utilization. 6LoBAC is a format that represents the MSDU of IPv6 over the MS/TP body. Furthermore, IPV6 for MS/TP interfaces refers to the inclusion of link-side bargaining interface identifiers. For security purposes, all-comprehensive viewing addresses (MAC address-derived desktop interface identifiers) supply an association with possibilities for governing address scanning. The author of [22] has suggested that each universally seen address originates from a 64-bit semantically interface identifier.

### 5.5.5 IPv6 over DECT/ULE

The UltraVo Energy (UEL) standard constituted low-energy interface technology using the digital enhanced cordless telecommunications (DECT Forum), which is defined by the European Telecommunication Standards Institute (ETSI). Low-bandwidth smart sensor devices for home automation systems required DECT. Authors of [29, 32, 36, 37] defined IPv6 map above DVT Uly.

The DECT UEL protocol stack is represented in Fig. 18, where the MAC layer combines conventional DECT circuit mode operation and an updated UL packet mode operation. To conclude, DECT UL data link control (DLC) combines multiplexing, fragmentation, and reassembly for long packets from higher layers. Additionally, it runs each message verification. 6 LoWPAN criteria of IPV6 provide for abbreviating address, which takes revival form and title abbreviations to reduce burden.



Fig. 18 The DECT ULE protocol stack

Software-defined logically connected permanent virtual circuit (PVC) between FP (entrance to DECT fixed portion) and PP (DECT portable portion or 6 LN) generates data transmission over DECT UL, where FPs and PPs are set for once. Thus, start the dynamic connection of data trading and address setup of IPv6.

The link-layer of DECT ULE merged with Message authentication code with cipher block link (CBC- MAC) mode is [22, 39] for safety purposes. The encryption and authentication messages also depend on AES128. A master user authentication key (UAK) generates during the establishment of DECT ULE. The DECT Standard Authentication Algorithm 2 (DSAA2) builds the session security key and the master authentication key. DECT ULE is a modern innovation created for distinctive IoT utilization cases like domestic, office, and mechanical mechanization, control and observing frameworks, medical care, and security systems.

### 5.5.6 IPv6 over 802.11ah/Wi-Fi

The IEEE 802.11ah standard makes a difference in spare transmission control by developing the Sub-1 GHz recurrence band. It is suitable for IoT for three significant features:

- Supports numerous gadgets in a single basic service set (BSS)
- Provides energy-saving innovations
- Empowers remote stations to switch from prominent mode to additional control

Since 802.11ah can be a low-power/low-rate innovation, MAC communication sessions get considered as crucial productivity. This fact led to the introduction of the 6 LoWPAN invention [29, 41] to effectively transmit IPV6 datagrams through IEEE 802.11ah remote networks.

The BSS and stations (STA) create through an Access Point (AP) of the framework. The 802.11ah bus can include STAs, where maximum STAs are in rest mode and a surplus of these can occasionally check for beacon-frame infections including site traffic indication map (TIM). Additionally, the 802.11ah compresses the film-level topology and accepts that the STA maintains a network in the AP where all communication within the STA passes over the AP. IEEE 802.11ah 2 does not revert to the topology in layer 2. The combination of the PHY layer (802.11ah), the 802 coherent connected layer, and the MAC layer (802.11ah) creates the WLAN convention stack. The IPv6 combines with 802.11ah via LLC, as shown in Fig. 19.



Fig. 19 Protocol stack for IPv6 over 802.11ah

## IPv6 over 802.11ah Protocol Stack

Utilizing the 6LoWPAN hub, which is a 6LoWPAN Hub (6LN) and 6LoWPAN Border Router (6LBR), are connected within the same gadgets having 802.11 properties. Ordinarily, in an 802.11ah star topology, the practical of 6LBR is given on the AP [40]. 6LNs are connected with STAs and communicate with 6LBR utilizing an 802.11ah association; for this reason, the 802.11ah MAC layer does not characterize work topology; it is advised that the 6LBR is the sole routing system handy inside the company. Subsequently, there are no 6LoWPAN switches (6LR). Additionally, considering security issues, the functionalities characterized in [37], then upgraded in [29] can also be accepted substantially for the 802.11ah case.

## 5.6 *IoHT Wireless Protocols: 5G*

The primary stage of 5G details is characterized in Release 15-3GPP. The design of 5G is a modern discussion interface that bolsters heterogeneous access systems and handles variable transmission capacities. Bundle center arrange overhauls are moreover actualized, where conventional and portable administrations share a framework (cloud information centers) for benefit conveyance and operational efficiency. The frequency range is divided for different bands:

- Low band: 600–700 MHz
- Mid-band: 2.5–3.7 GHz
- High band: 25–39 GHz

Higher frequencies can reach up to 80GHz. Range and frequency bands are correlated with each other. The 4G range is homogeneous to the low-band 5G range; 5G covers almost 1.5 km range. Data rate has low-band download speeds slightly higher than 4G per minute, with mid-band permitting speeds of 100–900 Mbps. Downloading speeds of high band and higher frequencies accomplish 1–3 Gbps per minute.

The convoluted encryption system is stronger than 4G, and it is also multi-layer and multi-criteria approach-dependent. For the most part, the level of 5G security is uncharacterized by the number of indicated security components. A multi-stakeholder approach that includes administrators, merchants, controllers, arrangement producers, and agents of 5G endorsers (from diverse biological system sections) is crucial to the security pattern of reliable, cost-efficient, and sensible 5G networks. Desires are that 5G will grow boundaries in all areas of present-day life, such as traveling, driving, generation productivity changes, keen framework arrangement like close cities with close homes, buildings, clinics, industrial facilities, open security, administration, etc. The tiny cell structure of 5G systems moves forward the indoor scope compared to other cellular communication advances and, at the same time, impacts the advancement of diverse HD undertaking

administrations, domestic VR, holographic communication, telemedicine, and other unused services.

### **5.7 IEEE 802.16 (WiMAX)**

WiMAX innovation is based upon the IEEE 802.16 standard, empowering the conveyance of remote broadband administrations anytime, anyplace. WiMAX items can suit settled and versatile utilization models across a wide range of applications. The IEEE 802.16 standard was created to convey the non-line-of-sight (NLoS) network between a supporter station and a base station. IEEE 802.16 innovation has been put forward to overcome the disadvantages of WLANs and to generate versatile systems. It gives distinctive QoS planning for supporting heterogeneous activity counting bequest voice activity, VoIP (voice over IP), voice and video streams, and web information activity. The conspicuous highlights of WiMAX incorporate quality of benefit, high-speed web, office over a long remove, versatility, security, and mobility. The WiMAX forum is a nonprofit organization formed to promote the adoption of WiMAX-compatible products and services, implemented for 50 km area coverage with a maximum of 5.8 GHz at 1Gbits/s with high power in PMP topology for WirelessMAN.

Diverse security arrangements are empowered in WiMAX systems, like the Advanced Encryption Standard (AES) with a 128-bit key: Rivest, Shamir, and Adelman (RSA) with a 1024-bit key and Triple Data Encryption Standard (3-DES). Both AES and 3-DES are symmetric encryption calculations employing a block-cipher strategy, whereas Rivest, Shamir, and Adelman (RSA) is an asymmetrical algorithm.

The discussed interface in IEEE 802.16 systems is secured by confirmation strategies, secure key trade, and epitome. By typing information from authorized clients, the base station limits unauthorized client access. Other than that, it supports the privacy key management (PKM) convention to secure two-layer key dispersion and trade, as well as real-time affirmation of subscribers' recognizable proof, which guarantees secure remote information transport. WiMAX pertinence is recognized in remote MAN arrangement, provisioning of web network and generic client applications, natural checking, keen cities, telemedicine, etc.

### **5.8 Highway Addressable Remote Transducer (HART)**

The HART convention employs the frequency-shift keying (FSK) standard to superimpose advanced communication signals at a moo level on the best of the 4–20 mA. This empowers two-way field communication to take place and makes it possible for extra data beyond what is normally associated with the ordinary preparing variable to be communicated from a smart field instrument [22]. Obtaining a frequency of

2.4 GHz covers an area of approximately 200 m and a low-power draw for Star and Mesh topology based on the hub or gateway transmission data rate of 250 kbps.

Communications are continuously scrambled in a HART organize. The arrange employs a 128-bit AES encryption framework. The security chief within the wireless HART gateway regulates three parameters: organize ID, connect key, and session key. In addition, a common arrange key is shared among all gadgets organized to encourage broadcast movement as required. A partitioned 128-bit connect encryption key is utilized to keep sending and receiving information privately, amid the joining period, where encryption cannot be disabled.

Ordinary HART use cases are prepared industry checking (prepare car generation, chemical portions, nourishment and refreshment, control era), handle optimization, security improvements, environment and well-being checking, upkeep optimization, etc.

### ***5.9 ISA100.11a: Low Data Rate Network***

ISA 100.11a low data rate network is upheld with expanded security and framework administration levels. In compliance with best hones, the ideal number of hubs within an arrangement is 50–100. The International Society of Automation (ISA) a non-profitable organization of technocrats in industrial automation that controls the ISA100.11a standard designed for covering approximately 100 m with 2.4GHz frequency, which draws low power in the Star or Mesh topology.

ISA 100.11a standard is implanted with integrity checks and optional encryption at the data link layer of the OSI model. Besides, security components include in the transport layer. Also, 128-bit keys use in transport and information connect layers. A shared worldwide key, a private symmetric key, or certificate is vital for a sensor hub to connect an ISA 100.11a network.

The foremost imperative use cases are solid checking and alarming, resource administration, prescient upkeep, observing condition, open-circle control, and closed-circle control mechanical applications.

### ***5.10 LoRaWAN<sup>®</sup> Specification v1.1***

LoRa gives remote, low-cost, and secure bidirectional communication for the Internet of Things (IoT) applications. Deployed for battery-powered end devices, the LoRaWAN<sup>®</sup> network protocol is optimized. LoRaWAN<sup>®</sup> Detail v1.1 includes support for handover meandering, Lesson B, and security enhancements. File points of interest LoRa is optimized for long-range communication, has low control utilization, and is designed to support large-scale deployment. LoRa is built with Semtech's LoRa tweak conspire. Moreover, LoRa is the PHY layer for an LPWAN innovation that employs chirp spread range to send information from one point



to another. LoRaWAN differs from LoRa – it could be a media access control (MAC)-layer convention built on the beat of the LoRa PHY layer. This protocol is a radio frequency of license-free sub-gigahertz bands, such as 433 MHz, 868 MHz, 915 MHz, and 923 MHz. A Star topology has a coverage area of 30 km with 50Kbps transmission rate.

Normally, LoRa use cases are control metering, water stream, gas or comparative quantitative observing; coordination and checking transportation; keen domestic, office, and smart city apparatuses; detecting contamination naturally, flooding, torrential slide, and timberland fires; savvy security frameworks, agribusiness, and mechanical automatization; and low-cost private systems with humble throughput necessities as an elective to commercial networks.

## 6 Routing Protocols

In order to deal with the restrictions of IoT frameworks, a directing convention ought to meet particular prerequisites and utilize distinctive techniques [42]. Such a convention should coordinate the activity design of its sending region and be resourceful in terms of control utilization. Moreover, it must scale in terms of memory and execution while also being able to deal with scanty area changes. Also, an IoT directing convention is required to recognize and maintain a strategic distance from one-way joins and be preservationist on the transmitter vitality utilization. Final but not slightest, supporting IPv6 and versatility are considered fundamental qualities. The techniques utilized incorporate proactive steering by attempting to have a worldwide visualization of the full organized topology at all times, as well as receptive steering and demand for seeking different routes. Table 2 shows a scientific categorization of the foremost imperative steering protocol in the IoT domain [22].

### 6.1 RPL

In 2012, the vector routing protocol for low-power and lossy network (RPL) is extricated by IETF, information collected from [43]. The Destination-Oriented Directed Acyclic Graph (DODAG) originated from the RPL to obtain a one way from each hub scale to the root. The hub sends complete venture to the source. Furthermore, the source selects a Destination Advertisement Object (DAO) from a hub that ought to communicate. Further, it handles the hubs DODAG Information Sales (DIS) demands that need to connect with the arrangement. RPL hubs can be displaced by keeping track of these patterns in the primary format.

**Table 2** A scientific categorization of the foremost imperative routing protocol in the IoT domain

Routing protocol name	Strategy	Mechanism	Algorithm	Traffic type	Main features	IPv6 support	IoT routing challenges met	Disadvantages
RPL	Proactive	Energy-aware metrics and multipath routing	Distance vector and source routing	MP2P, P2MP, and P2P	(i) Loop detection and avoidance (ii) Self-configuration (iii) Timer management	Yes	(i) Local and global repairs (ii) Energy usage low (iii) Mobility (iv) High scalability (v) Low memory usage	Not encrypted
CORPL	Proactive	Energy-aware metrics and multipath routing	Distance vector	MP2P, P2MP, and P2P	Opportunistic forwarding approach based on RPL	Yes	Data management and server technologies	No security and storage management
P2P-RPL	Reactive	Energy-aware metrics and multipath routing	Distance vector and source routing	P2P	Discovers the best-quality route for any source-destination pair	Yes	(i) Local and global repairs (ii) Energy usage low (iii) Mobility (iv) High scalability	No security and high memory required

(continued)

**Table 2** (continued)

Routing protocol name	Strategy	Mechanism	Algorithm	Traffic type	Main features	IPv6 support	IoT routing challenges met	Disadvantages
LoadNG	Reactive	Energy-aware metrics	Distance vector	P2P	(i) A lightweight variation of AODV (ii) Suitable for a more general traffic pattern	Yes	(i) Energy usage low (ii) Mobility (iii) High scalability (iv) Low memory usage	High delay in the route discovery and no security for local repair.
CARP	Reactive	Energy-aware metrics and multipath routing	Link state	MP2P, P2P, and P2MP	(i) Link quality selection for packet forwarding (ii) High packet delivery ratio for increasing traffic	Yes	Data management and storage management	(i) No security (ii) No server technologies (iii) No reusability of previously collected data

Reprinted from “Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends,” by A. Triantafyllou, P. Sargiannidis, and T. D. Lagkas, 2018, *Wirel. Commun. Mob. Comput., Volume* (2018)

## 6.2 *RPL Enhancements*

There are multiple proposals for conducting basic RPL conferences. One of the most standard point-to-point responsive RPLs (P2P-RPL) is P2P-RPL, which requests single or multiple routers to search paths within an LLN [44]. In IoT sector, energetic RPL (D-RPL) is utilized in advanced IoT devices for its vitality proficiency to organize end-to-end delay. MRPL is the portable form of RPL that focuses on portability administration in IoT situations [45]. However, it ignores unnecessary handovers and unreliable associations for some cases. Also, a “smart-HOP” conversion of MRPL was proposed for multifaceted optimization in RPL, known as MRPL.

## 6.3 *CORPL*

For cognitive radio-capable AMI networks, CORPL is a routing protocol that can be a nonstandard extension of RPL built for cognitive systems and uses the DODAG topology era. It is anticipated that smart grid communication uses cognitive radio, which will be essential in future aspects. CORPL employs information transmission to forward the bundle by choosing numerous forwarders (forwarder set) [46]. It arranges them to select the ideal another bounce to hand-off packets. DODAG is designed similarly to RPL. By utilizing the DAG information question (DIO) messages individually, the hub keeps a sending set rather than its previous primary set and illuminates its neighbor with its changes. By following the up-to-date data, each hub powerfully overhauls its neighbor’s needs to construct the forwarder set.

## 6.4 *Channel-Aware Routing for IoT*

Channel-aware routing protocol (CARP) uses logical quality data for cross-layer hand-off assurance, in which hubs are chosen for transferring problems if their neighbors have a history of effective bugs. CARP integrates the quality of the interface with direct topology data (bounce tally), so the network can take courses around voids and shadow regions.

CARP may be a separated distributed steering convention used in underwater wireless sensor networks (UWSN) [47]. Its resources incorporate conveying bundles of reasonable time with moderate vitality. In expansion, it can connect with previous data points that are calculated from chronically exchanged fruitful information. The history is collected from adjacent sensors in arranging to select the sending hubs.

The biggest disadvantage of CARP is that it does not allow the reuse of already collected data. E-CARP significantly reduces communication difficulties by improving the CARP identification capability, which allows the sync hub to release

already received information about sensors. The Internet of Underwater Things is associated with E-CARP, which is defined as an energy-efficient routing protocol for UWSNs [48], which initiate an affordable packet of energy consumption protocol to enhance the innovation of enormous unexplored ocean volume.

## 7 IoHT Service and Low-Power and Lossy Network IoT Applications

This is often intrinsically energetic and can be effortlessly upgraded by including extra administrations with particular highlights and various applications covering both single and clustered-condition arrangements. This segment presents each of the administrations and applications depicted in Fig. 20.

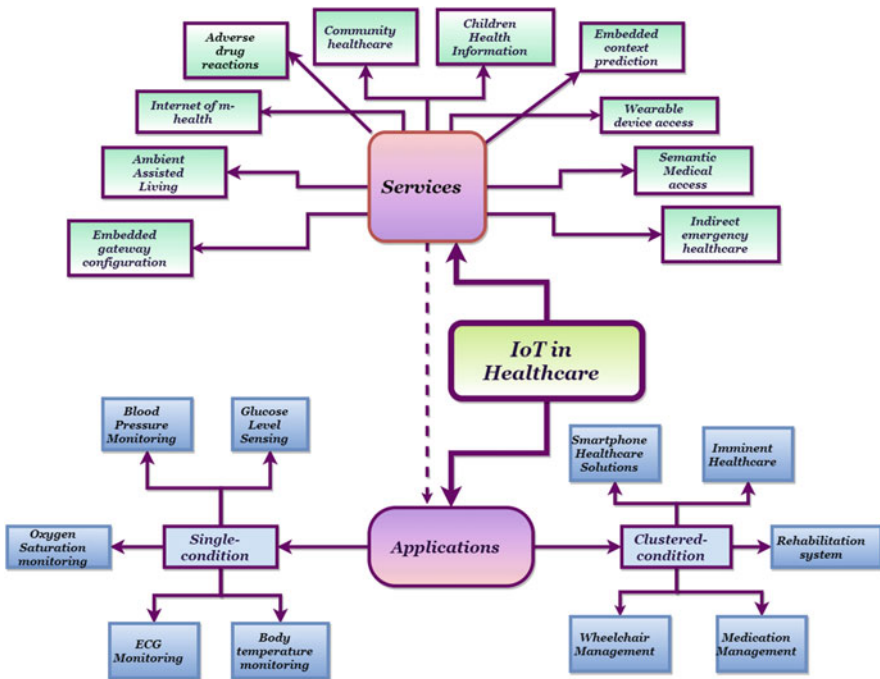


Fig. 20 IoT healthcare services and applications

### **7.1 *Ambient Assisted Living (AAL)***

An IoT platform powered by artificial intelligence that can address the medical care for the aged and disabled person is referred to as a supportive lifestyle or ambient assisted living. These structures are designed for supporting old age and incapacitate people. The authors of [15] mentioned that a combination of keep-in-touch standard technology and closed-loop healthcare administration can encourage AAL, which is appreciated for the key features of AL worldview with IoT. For this reason, researchers have given concentration for generating smart packages of objects and closed-loop healthcare services function through the IoT. A secure plus adaptable stage-based IoT and cloud computing protocol has been proposed [46].

### **7.2 *Community Healthcare (CH)***

This may be an IoT-based arrangement around civilian clinics, private areas, or provincial communities. The series connection of several systems can be realized as a satisfactory arrangement. In this regard, the collection of special prerequisites of assembly is inevitable, which creates special interests in community welfare. The structure of community treatment institutions can be regarded as “virtual rehabilitation centers.” Depending on a useful system of a four-layer structure that has been considered for a resident health information service platform, a strategy for sharing information between therapeutic offices includes the benefit stage for obtaining well-being records and inaccessible restorative counsel [33].

### **7.3 *Adverse Drug Reaction (ADR)***

It might be harmful to human beings by taking medicine for an adverse drug reaction. Since the ADR is inalienably nonexclusive, that’s not particular to the pharmaceutical for a particular infection; there must be an independent plan for certain common specialized issues and their solutions. Here, the patient’s terminal recognizes the sedate by implies of barcode/NFC-enabled devices. With the assistance of a pharmaceutical smart data framework, this data is at the point to facilitate the sense of whether the sedate is congruous with its hypersensitivity profile and electronic well-being record, or not.

#### **7.4 *The Internet of m-Health Things (m-IoT)***

m-health is nothing but versatile computing, therapeutic sensors, and communications that progress for healthcare organizations for IoT healthcare administrations; it is worth noting that there is an existence of a few particular highlights inherent in the worldwide portability of partaking substances [49]. Moreover, m-IoT administration leads that conception. Context-aware issues and m-IoT environments are two unmistakable challenges in m-IoT administrations.

#### **7.5 *Wearable Device Access (WDA)***

In this setting, a promising feature called wearable gadgets is required. It is related to a movement of recognition strategies based on portable gadgets for further diagnosis of patients [50]. The use of IoT-based accessible action can check frameworks and addresses, which represent how Bluetooth can strengthen WBANK for less lively wearable gadgets. [52].

#### **7.6 *Children Health Information (CHI)***

According to the needs of children and their family members, it is important to focus on children's well-being and develop a common open space for children's motivational, behavioral, or mental health problems. The dedicated IoT management department is called Child Health Information (CHI) persuaded to establish a strong way to meet this demand. In this way, an intuitive symbol is set in the pediatric ward that focuses on training, entertaining hospitalized children [44], and IoT-based m-wellbeing administrations that may urge young teachers to achieve excellent health and parental support [51].

#### **7.7 *Semantic Medical Access (SMA)***

People have considered the use of semantics and ontology to share large amounts of recoverable data and information. The IoTs require a partitioning facility called semantic medical access (SMA) to set up recovery semantics and ontology [11]. The Internet of Things medical applications use a restorer running display engine to analyze information about a large number of sensors stored in the cloud.

### **7.8 *Embedded Context Prediction (ECP)***

To create context-aware healthcare applications in IoT systems, third-party engineers need tedious systems with appropriate tools, which can be called embedded context prediction (ECP) that predicts benefits [55].

### **7.9 *Embedded Gateway Configuration (EGC)***

The advantages of implantable gateway settings are building the interface that can be arranged with hubs, web, and other therapeutic hardware. The advantage here is that computerized inspections can be done like an ECG machine.

### **7.10 *Indirect Emergency Healthcare (IEH)***

Healthcare issues are extremely important in many emergencies, including adverse weather conditions, traffic accidents, landslides, or fires. Research on these topics in emergency medical care based on the IoT network is extremely valuable.

## **8 IoT Healthcare Applications**

When extending to IoT management, IoT applications deserve further consideration. Therefore, management is developer-centric, while applications are user-centric. These projects can be seen as advancements in the Internet of Things, which can lead to different healthcare arrangements.

### **8.1 *Measuring Glucose Levels***

Diabetes can be a bunch of metabolic infections in which high blood sugar levels persist for a long time. In this strategy, sensors from quiet environments are connected to important healthcare providers through IPv6 associations [56].



## **8.2 *Blood Pressure Monitoring***

By showing the communication structure between the medical station and the medical center, an incentive scheme must be remotely controlled BP regularly [57]. It proposes a device for BP data collection and transmission on the IoT network. A portable BP monitoring is based on the Internet of Things.

## **8.3 *Electrocardiogram Monitoring***

The observation of the electrocardiogram (i.e., the electrical activity of the heart recorded by the electrocardiogram) fuses the assessment of direct pulse and the assurance of the fundamental rhythm, just like the assurance of polyhedral arrhythmia, myocardial ischemia, and drawn-out QT break. System organizing looks at computerization methodologies to recognize irregular data with the goal that heart function can be recognized in real time. Also, the application layer for ECG monitoring in the IoT network includes a comprehensive ECG signal detection algorithm.

## **8.4 *Oxygen Saturation Monitoring***

The research of CoAP-based health care authorities talked about the function of pulse oximetry based on IoT [58]. The heartbeat oximetry method is suitable for noninvasively and continuously watching blood oxygen [59]. The potential of wearable heartbeat oximeter wrist OX2 is to pass Nonin. The availability of this machine depends on a good Bluetooth gadget profile, and the sensor can directly reach the Monere level. Also, just like telemedicine procedures, the machine can be used to continuously display the health of the affected person through the Internet of Things network. The wearable heartbeat oximeter that can observe and utilize the wireless sensor network can be adjusted according to the IoT community [60].

## **8.5 *Medication Management***

An intelligent packaging method is based on the Internet of Things drug management cabinet [61]. The method includes I2Pack and iMedBox prototype systems, the packaging method with controlled sealing of layered materials based on wireless communication control. The prototype implementation is shown here, and the ubiquitous drug control system is specifically designed to provide an AAL solution [61].

## **8.6 *Rehabilitation System***

The Internet of Things has the potential to enhance rehabilitation systems to alleviate problems associated with aging population and shortage of health experts. The literature proposes an ontology-based automated design method for an intelligent rehabilitation system based on the Internet of Things [62]. There are many rehabilitation systems based on the Internet of Things, such as prison-integrated application system, rehabilitation training for patients with hemiplegia, smart city medical rehabilitation system, and language training system for children with autism for learning languages.

## **8.7 *Wheelchair Management***

Numerous analysts have given themselves to create keen wheelchairs with completely robotized capacities for the impaired. The plan comes with WBAN coordinates with different sensors whose capacities are custom-fitted to IoT prerequisites [63]. Another notable example of wheelchair development based on the Internet of Things is a connected wheelchair designed by Intel's Internet of Things division.

## **8.8 *Healthcare Solutions Using Smartphones***

Today, the rise of electronic products with smartphone control sensors highlights the rise of using smartphones as the driving force of the Internet of Things. Various computer program items are outlined to make smartphones flexible in healthcare tool, such as effectively conducting an extensive review of healthcare applications for smartphones and calculating dialog boxes for patients and general healthcare applications [64], as well as dialog boxes for treatment guidance, preparation, data search applications, etc. The safe reference application regularly gives the name of the drug and its logo, measurement, cost, and identification focus.

# **9 IoT Healthcare Security**

Consequently, the IoT medical care space might be an objective of aggressors. To encourage a choice of using IoT in the healthcare field, from the perspective of medical services, it is vital to identify and investigate the clear highlights of IoT security and protection, including security prerequisites, weaknesses, risk models, and countermeasures.

## ***9.1 Confidentiality***

Medical information for unauthorized users must be obstructed, which is ensured by confidentiality. Additionally, secret data is illegal to reveal its substance to eavesdroppers.

## ***9.2 Integrity***

An adversary does not alter received medical data, ensured by integrity, and also the integrated store data and contents must be encrypted.

## ***9.3 Authentication***

The end-to-end communication is verified by authentication.

## ***9.4 Information Freshness***

Data freshness includes critical information. Since every IoT healthcare network provides some metrics that change over time, it is necessary to ensure that every message is up to date. Data freshness means that every data set is up-to-date and ensures that no opponents replay old news [69–71].

## ***9.5 Non-Repudiation***

The hub cannot refuse to send previously sent messages that indicate non-repudiation.

## ***9.6 Authorization***

Authorization assures that network services or resources allow access only to authorized nodes [72, 73].

## **9.7 Resiliency**

In any compromise between interconnected devices, the network system should be encrypted to prevent any attacks [74–77].

## **9.8 Error Limitations**

If there is failure, for example software error, a device compromise, and failure of a device, the safety program should continue to provide corresponding safety services.

## **9.9 Self-Protection**

It is possible to malfunction or run out of energy of the medical devices in the IoT healthcare network; if this happens, then the lowest level of security gets access from the remaining or cooperating devices.

# **10 Security Challenges**

## **10.1 Computational Limitations**

IoT health devices have embedded low-speed processors. The central processing unit in such equipment is not very powerful in terms of speed. Computationally expensive operations are unable to run on these devices.

## **10.2 Energy Limitations**

Usually small and low-power battery medical devices are used for IoT Health networks. When there is no need to report sensor readings, such devices save energy by turning on the power-saving mode.

## **10.3 Dynamism**

Information from medical equipment is unpredictable, such as wearable temperature sensors or heart rate monitoring gadgets, because they are connected to the Internet

and cannot provide inconsistent data over time. Different networks occupy different security configurations and settings. Therefore, it is very important to observe the IoT device information for  $24 * 7 * 365$  days.

### ***10.4 Scalability***

A large number of devices are interconnected to the global information network due to the enhancement of IoT devices. Therefore, it will be a difficult task to plan an adaptable safety plan without compromising the necessity of safety.

### ***10.5 The Multiplicity of Devices***

The health devices in the IoT health network are diverse for transmitting data from PCs to low-end RFID tags. Therefore, the challenge is to design a security solution that can accommodate even the simplest equipment.

### ***10.6 A Dynamic Network Topology***

The temporal and spatial access characteristics of medical equipment make the network topology change dynamically.

### ***10.7 A Multi-Protocol Network***

Through the proprietary network protocol, the health device can communicate with other devices on the local area network. Also, in the IP network, the same IoT device can communicate with the IoT service provider. Therefore, it is very difficult for security experts to obtain reliable security.

### ***10.8 Data Privacy and Security Updates***

The security system must be updated to mitigate important vulnerabilities. Therefore, IoT health devices should contain updated security patches.

## 11 Future Aspects

IoT in healthcare is a structure of sensors that can gather significant well-being data all over the place and offer it through a safe organization. A cycle gathers data to identify any irregularities, so if any irregularities are discovered, then an admonition will be created. Another computerized stage for persistent observing and determination is Medicine 4.0 controlled by IoT. IoT in healthcare contains different structures utilizing diverse figuring standards. ML, edge registering, and the latest advances like SDN blockchains implemented these designs. To accomplish ideal organization and administrative execution, the capacities of ML are abused in various use instances of IoT in healthcare.

To predict the patient's condition and determine abnormal behavior in real time, big data analysis provides a framework. By introducing a transparent and secure method of information and delivery, big data analysis can enhance data storage capabilities. The introduction of the separation of data and network management planes can enhance functions, and under the license of SDN, the network can be maintained more flexibly [65].

To prevent the far-reaching appropriation of IoT in healthcare structures, numerous genuine challenges have been distinguished; however, there are a few novel arrangements to lighten these challenges. The substantial Internet is a major change in the communication method of IoT in healthcare, which opens up new paths for healthcare. Through careful study of brochures and market models, a huge range of IoT in healthcare will inevitably be received.

In a nutshell, the impact and importance of IoT are highly elevated and undeniable, even though the effect of wireless technology on the human body [66] due to harmful radiations, which cause diseases like male infertility, brain tumor, hearing impairment, abnormal fetus, blurred vision, etc., is still debatable among some researchers. Hopefully, further invention and novel research on the IoT healthcare protocol will not only overcome associated drawbacks but also establish new horizons.

## 12 Conclusion

To improve human life, the demand for IoT technology is increasing in various fields. In the past few years, researchers have paid more and more attention to the field of IoT healthcare to enhance the provision of healthcare by adjusting the potential of the Internet of Health Things. This chapter focuses on various aspects of IoT-based medical technology and introduces various medical network architectures and structures to help access; more specifically, attention has been shifted to the evaluation and identification of correct community encapsulation and routing protocols. Interoperability between IoT technologies is a prime concern of the Internet of Things. A realistic reality is that every network age that wishes to

participate in this computing paradigm must obtain improvements, such as IPv6 compatibility, and should aim to reduce power consumption.

Another key requirement is the need for embedded protection. Every generation and agreement contains many basic requirements for the Internet of Health Things. The upgraded proposed protocol can help bridge the performance gap in some cases. The Internet of Health Things is the future, and it is expected to build a strong network foundation by enhancing and upgrading the appropriate technologies that have been implemented. For scholars and professionals, this chapter will inspire them to develop further advancement and more effective network protocols, close current gaps, and solve important deficiencies.

## References

1. J.R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future internet: The internet of things architecture, possible applications and key challenges, in Proceedings of the 10th International Conference Frontiers of Information Technology FIT 2012, pp. 257–260, 2012, <https://doi.org/10.1109/FIT.2012.53>
2. J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, D. Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, 2014
3. R.P. Singh, M. Javaid, A. Haleem, R. Suman, Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **14**(4), 521–524 (2020). <https://doi.org/10.1016/j.dsx.2020.04.041>
4. D.J. Cook et al., MavHome: An agent-based smart home, in Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications. PerCom 2003, pp. 521–524, 2003, <https://doi.org/10.1109/percom.2003.1192783>
5. F. Nasri, N. Moussa, A. Mtibaa, Intelligent mobile system for healthcare based On WSN and Android. *Int. J. Comput. Trends Technol.* **12**(4), 187–192 (June 2014). <https://doi.org/10.14445/22312803/IJCTT-V12P137>
6. H. Viswanathan, E.K. Lee, D. Pompili, Mobile grid computing for data- and patient-centric ubiquitous healthcare, in 2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT), June 2012, pp. 36–41, <https://doi.org/10.1109/ETSIoT.2012.6311263>
7. I.M. Box et al., A health-IoT platform based on the integration of intelligent packaging, unobtrusive. *IEEE Trans. Ind. Inf.* **10**(4), 2180–2191 (2014). <https://doi.org/10.1109/TII.2014.2307795>
8. A. J. Jara, M. A. Zamora, A. F. Skarmeta, Knowledge Acquisition and Management Architecture for Mobile and Personal Health Environments Based on the Internet of Things, 2012, <https://doi.org/10.1109/TrustCom.2012.194>
9. B. Xu et al., Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Trans. Ind. Inf.* **10**(2), 1578–1586 (2014)
10. C. Doukas, Bringing IoT and Cloud Computing towards Pervasive Healthcare, 2012, <https://doi.org/10.1109/IMIS.2012.26>
11. G. Zhang, C. Li, Y. Zhang, C. Xing, J. Yang, SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors, in 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), 2012, October, pp. 238–243, <https://doi.org/10.1109/HealthCom.2012.6379414>
12. X. M. Zhang, N. Zhang, An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine, in 2011 International Conference on Computer and Management (CAMAN), 2011, May, pp. 1–4, <https://doi.org/10.1109/CAMAN.2011.5778905>

13. M. Sahebi, B. Bin Mohd, and A. J. Jara, A network Mobility Solution Based on 6LoWPAN Hospital Wireless Sensor Network (NEMO-HWSN), pp. 433–438, 2013, <https://doi.org/10.1109/IMIS.2013.157>
14. S. Imadali, A. Karanasiou, A. Petrescu, I. Sifniadis, EHealth Service Support In IPv6 Vehicular Networks, pp. 579–585, 2012
15. Q. Zhu, R. Wang, Q. Chen, Y. Liu, W. Qin, 2010 IEEE / IFIP International Conference on Embedded and Ubiquitous Computing IOT Gateway : Bridging Wireless Sensor Networks into Internet of Things, 2010, <https://doi.org/10.1109/EUC.2010.58>
16. N. Bui, N. Bressan, M. Zorzi, “Interconnection of Body Area Networks to a Communications Infrastructure: An Architectural Study,” 2012
17. M.F.A. Rasid, Embedded Gateway Services for Internet of Things Applications in Ubiquitous Healthcare, no. November 2015, 2014, <https://doi.org/10.1109/ICoICT.2014.6914055>
18. P. Swiatek, A. Rucinski, IoT as a service system for eHealth, in 2013 IEEE 15th International Conference e-Health Networking, Application and Services (Healthcom 2013), pp. 81–84, 2013, <https://doi.org/10.1109/HealthCom.2013.6720643>
19. M. Díaz, G. Juan, O. Lucas, A. Ryuga, Big data on the internet of things: An example for the E-health, in Proceedings of the 6th International Conference on Innovative Mobile Internet Services. Ubiquitous Comput. IMIS 2012, pp. 898–900, 2012, <https://doi.org/10.1109/IMIS.2012.198>
20. X. Wang, J. T. Wang, X. Zhang, J. Song, A multiple communication standards compatible IoT system for medical usage, in 2013 IEEE Faible Tension Faible Consommation. FTFC 2013, pp. 1–4, 2013, <https://doi.org/10.1109/FTFC.2013.6577775>
21. W. Wang, J. Li, L. Wang, W. Zhao, The internet of things for resident health information service platform research. IET Conf. Publ. **2011**(586), 631–635 (2012). <https://doi.org/10.1049/cp.2011.0745>
22. A. Triantafyllou, P. Sarigiannidis, T.D. Lagkas, Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. *Wirel. Commun. Mob. Comput.***2018** (2018). <https://doi.org/10.1155/2018/5349894>
23. M. Franceschinis, C. Pastrone, M.A. Spirito, C. Borean, On the performance of ZigBee Pro and ZigBee IP in IEEE 802.15.4 networks. Int. Conf. Wirel. Mob. Comput. Netw. Commun., 83–88 (2013). <https://doi.org/10.1109/WiMOB.2013.6673344>
24. O. Bello, S. Zeadally, M. Badra, Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT). Ad Hoc Netw. **57**, 52–62 (2017). <https://doi.org/10.1016/j.adhoc.2016.06.010>
25. D. Dujovne, T. Watteyne, X. Vilajosana, P. Thubert, 6TiSCH: Deterministic IP-enabled industrial internet (of things). IEEE Commun. Mag. **52**(12), 36–41 (2014). <https://doi.org/10.1109/MCOM.2014.6979984>
26. J.D.R. Nepomuceno, N.M.C. Tiglao, Performance evaluation of 6TiSCH for resilient data transport in wireless sensor networks. Int. Conf. Inf. Netw., 552–557 (2017). <https://doi.org/10.1109/ICOIN.2017.7899546>
27. L.A.N. Man, IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1 : MAC sublayer IEEE Computer Society, vol. 2012, no. April 2012
28. C. Bormann, L. Toutain, R. Cragie, IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header, April 2017, <https://doi.org/10.17487/RFC8138>
29. P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, September 2011, <https://doi.org/10.17487/rfc6282>
30. K. Pister, T. Watteyne, Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration, May 2017, <https://doi.org/10.17487/RFC8180>
31. ITU-T Study Group 15, Recommendation ITU-T G.9959: Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications, 2015
32. D. Dragomir, L. Gheorghe, S. Costea, A. Radovici, A survey on secure communication protocols for IoT systems, in 2016 International Workshop on Secure Internet of Things (SIoT), 2016, pp. 47–62, <https://doi.org/10.1109/SIoT.2016.012>



33. D. Whiting, R. Housley, N. Ferguson, Counter with CBC-MAC (CCM), September 2003, <https://doi.org/10.17487/rfc3610>
34. Y.-G. Hong, J.-S. Youn, D.-K. Kim, J.-H. Choi, Transmission of IPv6 Packets over Near Field Communication: draft-ietf-6lo-nfc-17. Internet Engineering Task Force, 2020
35. ETSI, ETSI TS 102 939-1 V1.2.1 (2015-03) – Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network, vol. 1, no. phase 1. The European Telecommunications Standards Institute, 2015
36. S. Chakrabarti, E. Nordmark, C. Bormann, Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), November 2012, <https://doi.org/10.17487/rfc6775>
37. G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, September 2007, <https://doi.org/10.17487/rfc4944>
38. S.K. Das, D.J. Cook, A. Battacharya, E.O. Heierman, T.-Y. Lin, The role of prediction algorithms in the MavHome smart home architecture. *IEEE Wirel. Commun.* **9**(6), 77–84 (December 2002). <https://doi.org/10.1109/MWC.2002.1160085>
39. P. Mariager, Z. Shelby, M. Van de Logt, D. Barthel, Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE), May 2017, <https://doi.org/10.17487/RFC8105>
40. D.C. Vega, M. Robles, R. Morabito, IPv6 over 802.11ah: Draft-delpcarpio-6lo-wlanah-01. Internet Engineering Task Force, 2015
41. R.J. Robles, T. Kim, A review on security in smart home development. *Int. J. Adv. Sci. Technol.* **15** (2010)
42. G. Liang, J. Cao, W. Zhu, CircleSense: A pervasive computing system for recognizing social activities, in 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2013, pp. 201–206, <https://doi.org/10.1109/PerCom.2013.6526733>
43. K. Frank, P. Robertson, M. Gross, K. Wiesner, Sensor-based identification of human stress levels, in 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), March 2013, pp. 127–132, <https://doi.org/10.1109/PerComW.2013.6529469>
44. M. Sundholm, J. Cheng, B. Zhou, A. Sethi, P. Lukowicz, Smart-Mat: Recognizing and counting gym exercises with low-cost resistive pressure sensing matrix, in Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing – UbiComp'14 Adjunct, 2014, pp. 373–382, <https://doi.org/10.1145/2632048.2636088>
45. J.-C. Zhao, J.-F. Zhang, Y. Feng, J.-X. Guo, The study and application of the IOT technology in agriculture, in 2010 3rd International Conference on Computer Science and Information Technology, July 2010, pp. 462–465, <https://doi.org/10.1109/ICCSIT.2010.5565120>
46. A. Aijaz, H. Su, A. Aghvami, CORPL: A routing protocol for cognitive radio enabled AMI networks. *IEEE Trans. Smart Grid* **6**(1), 477–485 (2015, January). <https://doi.org/10.1109/TSG.2014.2324022>
47. S. Basagni, C. Petrioli, R. Petroccia, D. Spaccini, *Channel-Aware Routing for Underwater Wireless Networks* (May 2012). <https://doi.org/10.1109/OCEANS-Yeosu.2012.6263538>
48. Z. Zhou, B. Yao, R. Xing, L. Shu, S. Bu, E-CARP: An energy efficient routing protocol for UWSNs in the internet of underwater things. *IEEE Sensors J.* **16**(11), 4072–4082 (June 2016). <https://doi.org/10.1109/JSEN.2015.2437904>
49. R.S.H. Istepanian, E. Jovanov, Y.T. Zhang, Guest editorial introduction to the special section on M-health: Beyond seamless mobility and global wireless health-care connectivity. *IEEE Trans. Inf. Technol. Biomed.* **8**(4), 405–414 (December 2004). <https://doi.org/10.1109/TITB.2004.840019>
50. G. Sebestyen, A. Hangan, S. Oniga, Z. Gal, eHealth solutions in the context of Internet of Things, May 2014, <https://doi.org/10.1109/AQTR.2014.6857876>
51. M. Vazquez-Briseno, C. Navarro-Cota, J. I. Nieto-Hipolito, E. Jimenez-Garcia, J. D. Sanchez-Lopez, A proposal for using the internet of things concept to increase children's health awareness, February 2012, <https://doi.org/10.1109/CONIELECOMP.2012.6189903>

52. P. Lopez, D. Fernandez, A. J. Jara, A. F. Skarmeta, Survey of Internet of Things Technologies for Clinical Environments, March 2013, <https://doi.org/10.1109/WAINA.2013.255>
53. S.M. Riazul Islam, D. Kwak, M.H. Kabir, M. Hossain, K.-S. Kwak, The Internet of Things for health care: A comprehensive survey. *IEEE Access* **3**, 678–708 (2015). <https://doi.org/10.1109/ACCESS.2015.2437951>
54. S. Vicini, S. Bellini, A. Rosi, and A. Sanna, An internet of things enabled interactive totem for children in a living lab setting, June 2012, <https://doi.org/10.1109/ICE.2012.6297713>
55. G. Mantas, D. Lymberopoulos, N. Komninos, A new framework for ubiquitous context-aware healthcare applications, November 2010, <https://doi.org/10.1109/ITAB.2010.5687758>
56. R.S.H. Istepanian, S. Hu, N.Y. Philip, A. Sungoor, The potential of Internet of m-health Things ‘m-IoT’ for non-invasive glucose level sensing, August 2011, <https://doi.org/10.1109/IEMBS.2011.6091302>
57. J. Puustjarvi, L. Puustjarvi, Automating remote monitoring and information therapy: An opportunity to practice telemedicine in developing countries, 2011, [Online]. Available: <https://ieeexplore.ieee.org/document/6107349>
58. H.A. Khattak, M. Ruta, E. Eugenio Di Sciascio, CoAP-based healthcare sensor networks: A survey, January 2014, <https://doi.org/10.1109/IBCAST.2014.6778196>
59. A.J. Jara, M.A. Zamora-Izquierdo, A.F. Skarmeta, Interconnection framework for mHealth and remote monitoring based on the internet of things. *IEEE J. Sel. Areas Commun.* **31**(9), 47–65 (September 2013). <https://doi.org/10.1109/JSAC.2013.SUP.0513005>
60. E.C. Larson, T. Lee, S. Liu, M. Rosenfeld, S.N. Patel, Accurate and privacy preserving cough sensing using a low-cost microphone, in Proceedings of the 13th international conference on ubiquitous computing – UbiComp’11, 2011, no. 3, pp. 375–384, <https://doi.org/10.1145/2030112.2030163>
61. Z. Pang, J. Tian, Q. Chen, Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things, in 16th International Conference on Advanced Communication Technology, vol. 2, no. 6, February 2014, pp. 352–360, <https://doi.org/10.1109/ICACT.2014.6779193>
62. Y.J. Fan, Y.H. Yin, L. Da Xu, Y. Zeng, F. Wu, IoT-based smart rehabilitation system. *IEEE Trans. Ind. Inf.* **10**(2), 1568–1577 (May 2014). <https://doi.org/10.1109/TII.2014.2302583>
63. H.E. Gassara, S. Almuhammed, A. Moukadem, L. Schacher, A. Dieterlen, D. Adolphe, Smart wheelchair: Integration of multiple sensors. *IOP Conf. Ser. Mater. Sci. Eng.* **254**, 072008 (October 2017). <https://doi.org/10.1088/1757-899X/254/7/072008>
64. A.S.M. Mosa, I. Yoo, L. Sheets, A systematic review of healthcare applications for smart-phones. *BMC Med. Inform. Decis. Mak.* **12**(67) (July 2012). <https://doi.org/10.1186/1472-6947-12-67>
65. Y.A. Qadri, A. Nauman, Y. Bin Zikria, A.V. Vasilakos, S.W. Kim, The future of healthcare internet of things: A survey of emerging technologies. *IEEE Commun. Surv. Tutorials* **22**(2), 1121–1167 (2020). <https://doi.org/10.1109/COMST.2020.2973314>
66. L. RSA, M. GA, Effects of wireless devices on human body. *J. Comput. Sci. Syst. Biol.* **9**(4), 119–124 (2016). <https://doi.org/10.4172/jcsb.1000229>
67. C. Alcaraz, P. Najera, J. Lopez, R. Roman, Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration? 2010, [Online]. Available: <https://www.nics.uma.es/biblio/citekey/calcaraz10>
68. Z.B. Babovic, J. Protic, V. Milutinovic, Web performance evaluation for internet of things applications. *IEEE Access* **4**, 6974–6992 (2016). <https://doi.org/10.1109/ACCESS.2016.2615181>
69. P.K. Maddikunta, T.R. Gadekallu, R. Kaluri, G. Srivastava, R.M. Parizi, M.S. Khan, Green communication in IoT networks using a hybrid optimization algorithm. *Comput. Commun.* **159**, 97–107 (2020 June 1)
70. F. Naeem, G. Srivastava, M. Tariq, A software defined network based fuzzy normalized neural adaptive multipath congestion control for the internet of things. *IEEE Transactions on Network Science and Engineering* **7**(4), 2155–2164 (2020 April 28)

71. B. Sharma, G. Srivastava, J.C. Lin, A bidirectional congestion control transport protocol for the internet of drones. *Comput. Commun.* **153**, 102–116 (2020 March 1)
72. G. Smart, N. Deligiannis, R. Surace, V. Loscri, G. Fortino, Y. Andreopoulos, Decentralized time-synchronized channel swapping for ad hoc wireless networks. *IEEE Trans. Veh. Technol.* **65**(10), 8538–8553 (2015 December 17)
73. Aiello F, Fortino G, Guerrieri A, Gravina R. Maps: A mobile agent platform for wsns based on java sun spots, in *Proceedings of the ATSN*. 2009 May, vol. 200, issue 9
74. Fortino G, Guerrieri A, Bellifemine FL, Giannantonio R. SPINE2: Developing BSN applications on heterogeneous sensor nodes. In *2009 IEEE International Symposium on Industrial Embedded Systems*, IEEE, 8 July 2009, pp. 128–131
75. C. Ma, W. Li, R. Gravina, G. Fortino, Posture detection based on smart cushion for wheelchair users. *Sensors* **17**(4), 719 (2017 April)
76. Fortino G, Guerrieri A, Bellifemine F, Giannantonio R. Platform-independent development of collaborative wireless body sensor network applications: SPINE2, in *2009 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, 11 Oct 2009, pp. 3144–3150
77. C. Savaglio, P. Pace, G. Aloï, A. Liotta, G. Fortino, Lightweight reinforcement learning for energy efficient communications in wireless sensor networks. *IEEE Access* **7**, 29355–29364 (2019 March 4)

# Affective Computing for eHealth Using Low-Cost Remote Internet of Things-Based EMG Platform



Žygintas Tamulis, Mindaugas Vasiljevas, Robertas Damaševičius, Rytis Maskeliunas, and Sanjay Misra 

## 1 Introduction

Healthcare has become difficult to manage due to ineffective and unsustainable healthcare services to meet the growing demands of restrictions on accessibility, especially due to COVID-19-related issues. A remote, Internet of Things (IoT)-based medical platform can offer a seamless platform to connect people to healthcare institutions [1]. The concept of IoT can bring a very high added value to healthcare applications focused on reading biosignals by integrating numerous technologies, such as data science, sensors, and wireless communication; smart homes [2], including concepts such as affective computing [3], which combines the achievements of artificial intelligence (AI); and embedded systems and psychology for developing novel methods of human-computer interaction (HCI) for many diverse applications such as assisted living and health [4], education [5], entertainment [6], robotics [7], and marketing [8]. The rapidly growing need for better healthcare systems in real-time, IoT sensor-based affective computing exploits human emotions detected using visual, audio, or biosignal analysis for implementing an affective loop to control computer systems and software applications. Although there are many ways to detect human emotion, facial countenances, such as smiles, are the most easily recognizable. The category theory claims that people

---

Ž. Tamulis · M. Vasiljevas · R. Damaševičius (✉)

Department of Software Engineering, Kaunas University of Technology, Kaunas, Lithuania  
e-mail: [robertas.damasevicius@ktu.lt](mailto:robertas.damasevicius@ktu.lt)

R. Maskeliunas

Department of Applied Informatics, Vytautas Magnus University, Kaunas, Lithuania

Faculty of Applied Mathematics, Silesian University of Technology, Gliwice, Poland

S. Misra

Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

U. Ghosh et al. (eds.), *Intelligent Internet of Things for Healthcare and Industry*,

Internet of Things, [https://doi.org/10.1007/978-3-030-81473-1\\_3](https://doi.org/10.1007/978-3-030-81473-1_3)

across the world similarly express six basic emotions: anger, disgust, enjoyment, fear, sadness, and surprise [9]. The 2D valence-arousal model classifies emotions based on their level of arousal and valence [10]. Valence is a measure of emotional gratification, and it is represented on the horizontal axis. Arousal is a measure of the activation level of emotion, and it is represented using the vertical axis.

Studies focused on deeper comprehension of cognitive processes behind human emotions include the research of brain activity (electroencephalography signals or EEG) and face muscle neuronal activity (facial surface electromyography, sEMG) [11]. EMG captures the electrical activity of the muscles. The signals are acquired using electrodes attached over the muscle of interest. Here, we focus on the analysis of facial EMG signals for emotion recognition. Facial EMG is a noninvasive method aimed to evaluate facial muscular activity indicating the emotional responses. Facial EMG signals can be captured even when subjects are not consciously aware of stimuli presented or when individuals are trying to hide their reactions [12]. The analysis of facial EMG data is challenging due to high dimensionality, non-stationary signals, high noise, and high intersubject variability [13]. Traditional neurocomputing methods employ averaging over multiple trials to eliminate random noise and enhance the useful signal, which often requires many hours of recordings. Useful applications of facial EMG reading also include fatigue recognition in lorry drivers [14], recognition of anxiety level in exposure therapy [15], evaluation of neurological conditions of patients [16], stress recognition in students [17], evaluating work-related stress and fatigue [18], monitoring depression [19], performing neuromarketing studies [20], or using an alternative channel of human-computer communication [21–23]. Recently, EMG measurements have been applied in industrial applications for measuring the comfort levels of industry workers and validating the ergonomics of designs [24]. For example, EMG signals have been used as a reference for evaluating product design related to firefighter occupational activities [25]. A study based on EMG was used to evaluate bar benders at a construction workplace and to find optimal height and grip arm distance of a worktable based on the measured perception of the workers [26]. As a result, the EMG-based studies can lead to designing ergonomically optimal workplaces and increasing worker safety and boosting their labor efficiency and output [26]. Fatigue evaluation of ergonomics of trolley design using surface EMG was considered in [27]. The effect of ergonomically designed workstations for carpet weaving using shoulder EMG was analyzed in [28]. Coutinho et al. [13] performed the detection of five appraisal checks (control, goal conduciveness, novelty, power, and pleasantness) using EEG and facial EMG signals, but the study could not detect EMG signals usable to detect appraisal checks. Kaiser et al. [29] found spontaneous facial reactions (SFRs) represented by muscle activation in forming three emotional expressions (happiness, fear, and anger) using EMG signals captured from 7-month-old infants, while angry faces did not reveal an unambiguous response. Perusquía-Hernández et al. [30] focused on detecting micro-smiles by recording surface EMG signals from a neutral face. They reported at least 90.2% accuracy. Riehle and Lincoln [31] compared smiling vs imitation of smiling in face-to-face communication using EMG signals. Guendil et al. [32] used multiresolution analysis

of physiological signals of EMG, respiratory (RESP), electrocardiography (ECG), and skin conductance (SC) for human emotion recognition. They used Morlet, Haar, Daubechies, Symlet, and wavelet transform to obtain the most important wavelet coefficients and combined feature vectors for each emotion. A support-vector machine (SVM) classifier reached an accuracy of 95%. Hess et al. [33] estimated the reliability of facial EMG to recognize affective reactions to image stimuli vs facial mimicry. Facial reactions to positive affective stimuli showed acceptable consistency. Facial reactions to negative emotions or imagery showed unsatisfactory internal consistencies. Latham et al. [34] employed multiple physiological measures (including facial EMG) to evaluate the affective reactions and regulation of 113 subjects reacting to valenced images. The participants showed emotion-consistent zygomatic and corrugator muscula activity. Perez-Rosero et al. [35] analyzed blood volume pulse (BVP), EMG, and galvanic skin response (GSR) signals acquired during eight affective states and reported an accuracy of 88.1%. Thompson et al. [36] used psychophysiological measures to capture facial EMG to detect muscle activity characteristic of immediate emotional responses to emoticons. The results showed enhanced smiling reduced frowning and higher arousal for messages having an emoticon, thus indicating that emoticons raised positive emotions. Kehri et al. [37] used wavelet packet transform for feature extraction and SVM for classification of three types of facial emotions, achieving classification accuracy of 91.66% on 12 subjects. Similarly, Orguc et al. [38] used features extracted by discrete wavelet transform (DWT) and SVM for classification of facial gestures from ten individuals. Lajante et al. [39] discussed the reliability of facial EMG research. Guo et al. [40] used convolutional neural networks (CNNs) embedded on mobile devices to recognize emotions in facial expressions in real time.

However, there are still many research problems unsolved. More research is needed to realize the potentials of surface EMG technology into a practical technique with an impact on industrial ergonomics [41]. There is still to develop new methods for identification and extraction of information in EMG signals from a limited number of trials. There are two main methods for emotion identification from the human face. The first method is based on image processing using face photos (or videos). Another method uses surface EMG and electrodes directly attached to the human face. As muscular potentials are acquired directly from muscles involved in forming the emotion-related face expressions, facial EMG is considered as one of the most suitable physiological signals for the detection of emotional expressions [42].

With the arrival of IoT and increasing health awareness, the applications of wearable ECG and EMG sensors have increased. Known commercial EMG reading technologies include NIA (Neural Impulse Actuator) developed by O CZ Technology, AFFECTIVA, NVISIO, Empatica E4, Microsoft Band 3, and eHealth kit for Arduino. All of these can be easily adapted to send signals to IoT networks [43]. A low-cost prototype for facial expression detection using four-channel facial sEMG signals is presented in [44]. The authors of [45] explored combining two head-mounted human-computer interaction devices for controlling these devices. Two EMG-based popular biofeedback emotional therapies were shown successfully

by [46]. Embedded solutions are often affected by a precision drop over time, which makes them not suitable for reliable emotion recognition [47].

In this chapter, we present our aim to develop and explore the methods necessary for the remote IoT-based, fault-tolerant structure, inspired by a framework by Tuan Nguyen Gia’s group [48], focused on recognition of externally expressive emotions (positive, neutral, negative) by using an EMG-based human-computer interface for affective computing applications. To induce an affective reaction, one needs to apply stimuli to the subjects. Here, we used visual stimuli induced by showing movie clips via a standard desktop computer monitor.

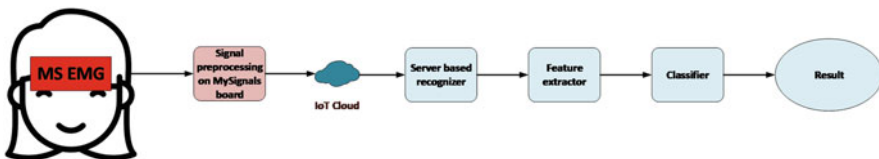
## 2 Methods

### 2.1 Outline

In this chapter, the following methodology is applied: IoT standalone data acquisition; data preprocessing and denoising; feature extraction, feature ranking, and dimensionality reduction; and classification. The methodology is summarized in Fig. 1.

### 2.2 Hardware

For data collection, we used MySignals [49]. MySignals is a low-cost generic IoT-based medical biosignal acquisition development platform that enables the acquisition of multiple physiological signals, including electrocardiography (ECG), electromyography (EMG), electrodermal activity (EDA), and many others (see Fig. 2; a version without a screen was used for sewing into the mask). We used the EMG sensor of the MySignals platform placed on surface muscles in the standard locations to record the bioelectrical activity from the muscles. Pre-gelled Ag/AgCl electrodes were used to attach electrode leads to the human body. The sampling rate of the EMG sensor is 1000 s<sup>-1</sup>. The bandwidth is 10–400 Hz, and the input voltage range is 0–3.3 mV.



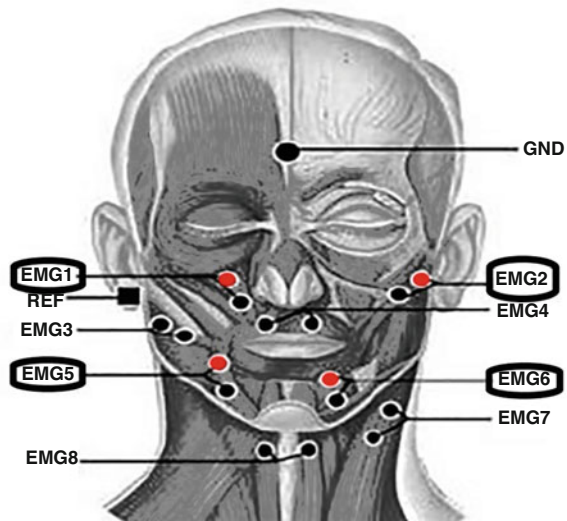
**Fig. 1** The main stages for remote IoT-based emotion recognition using facial IoT EMG sensors





**Fig. 2** MySignals platforms and sensors used for acquisition of EMG signals

**Fig. 3** Electrode placement locations. (Adopted from [50]). Red dots show the electrode placement locations used in this study



### 2.3 Data Acquisition

We used the electrode placement locations for facial EMG as suggested by Lopez-Larraz [50] (see Fig. 3). Due to the limitations of the MySignals platform (only four sensors can be used simultaneously), we only used the locations EMG1, EMG2, EMG5, and EMG6, further denoted as Channel\_1, Channel\_2, Channel\_3, and Channel\_4, and did not use other locations.



The locations are associated with levator labii superioris (EMG1), zygomaticus major (EMG2), depressor anguli oris (EMG3, EMG5), and depressor labii inferioris (EMG4, EMG6) facial muscles. The muscles have been associated with the expression of various emotions (happiness, zygomaticus major; disgust and surprise, levator labii superioris; sadness, depressor anguli oris) [51]. The placement is asymmetrical in order to acquire a more diverse set of signals (symmetrically attached sensors will yield correlated signals as healthy people are expected to have symmetrical facial responses to emotional stimuli). Sensors were sewn on a comfortable balaclava-style mask with a connection to a pocket-sized MySignals kit for remote IoT transmission.

## 2.4 Data Preprocessing

First, we used a fourth-order forward-backward band-pass Butterworth filter with the 10 and 450 Hz cutoff frequencies as suggested in [46]. Next, EMG data were denoised using the BoostEMD [52] denoising approach, which is based on the signal decomposition into intrinsic mode functions (IMFs), which are created using empirical mode decomposition (EMD) [53]. Denoising is performed by retaining the nonrandom IMFs and discarding the noisy IMFs. The data is normalized so that the minimum and maximum values of each window of data are mapped to zero mean and standard deviation of 1.

## 2.5 Feature Extraction and Reduction

For feature generation, we use the covariance matrix of the EMG channel data. The covariance matrix features capture the energy of the signal. The covariance matrix is calculated from channels in the observation matrix as follows:

$$\text{COV}(X, Y) = \frac{1}{N} \sum_{i=1}^N (X_i - \bar{X})(Y_i - \bar{Y}), \quad (1)$$

where  $X, Y$  are observations from any two EMG data channels.

For feature ranking, we adopt the two-sample t-test with pooled variance estimate as class separability criterion. The t-test statistic is calculated as follows:

$$t = \frac{\bar{x}_1 - \bar{x}_2}{s_P \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}}, \quad (2)$$

$$s_P = \sqrt{\frac{(n_1 - 1)s_1^2 + (n_2 - 1)s_2^2}{n_1 + n_2 - 2}}, \quad (3)$$

where  $x_1, x_2$  are observation samples,  $s_1, s_2$  variances, and  $n_1, n_2$  size of samples.

## 2.6 Classification and Evaluation

For classification, we apply the K-nearest neighbor (KNN) classifier. 80% of data is kept for training and 20% for testing. The process is repeated for 20 times using holdout cross-validation. Then, the experimental results are assessed using the mean values of the accuracy, F-score, and Kappa metrics. Here, accuracy is the ratio of correct predictions divided by the number of predictions. The F-score combines precision and recall and characterizes precision (the ratio of samples it classifies correctly) and robustness (it does not skip a large number of positive samples) of the classifier. Kappa compares a factual accuracy with an expected accuracy. It is computed as follows:

$$K = \frac{p_o - p_e}{1 - p_e}, \quad (4)$$

where  $p_e$  is random guessing and  $p_o$  is the accuracy of prediction.

To make sure that the differences between the obtained results are significant, we executed the McNemar test [54] at  $\alpha = 0.05$  level of significance.

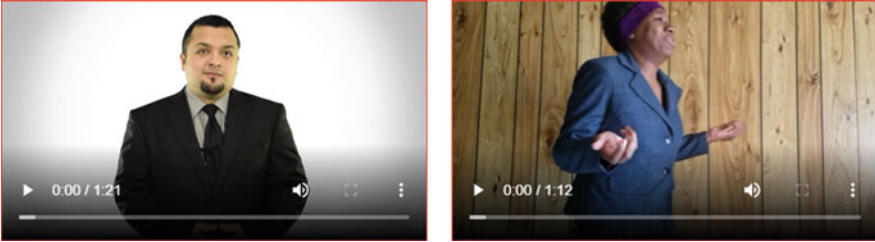
## 3 Results

### 3.1 Dataset

We used the One-Minute Gradual-Emotional Behavior dataset (OMG-Emotion dataset) [55]. The sample frame screenshots from the movie clips are presented in Fig. 4.

The clips correspond to expected neutral, positive, and negative emotional reactions. The emotional valence of the clips was confirmed by an experienced psychology expert specializing in emotional intelligence research. Hereinafter, the clips are labeled as “Clip 1,” “Clip 2,” and “Clip 3.” The first clip shows the grass near the sidewalk with no action. The second clip shows a playing kitten. The third clip shows a medical procedure.

We have collected data from 14 subjects (10 male and 4 female). All subjects were students at Kaunas University of Technology (mean age = 22 years, SD = 3.86). The subjects were free of any neurological or psychiatric disorder.



**Fig. 4** Sample shots from movie clips of One-Minute Gradual-Emotional Behavior dataset (OMG-Emotion dataset) [55] aimed to induce affective facial expressions

Informed consent was obtained. All ethical procedures were adhered to follow the requirements of the Helsinki Declaration. The EMG signals were processed using MATLAB software (version 8.1.0.604, R2013a).

### 3.2 Protocol

We followed the protocol described in [56] (see Fig. 5). Subjects were informed that they will be presented a sequence of visual stimuli on a PC monitor while they should stay as still as possible during the experiment. Each trial started with a 50 ms audio tone, which was succeeded by the visual stimuli 1 s later. Each stimulus was shown on the screen for 5 s, after which a blank (black) screen is shown for 6 s. Each subject viewed eight blocks (neutral, positive, negative) of visual stimuli presented in random order. Synchronization of visual stimuli with EMG signal recordings was implemented in Flash (using ActionScript 3) and JavaScript (using the JavaScript `play()` method).

### 3.3 Results

For calculations, a window of 1 s is used. The feature ranking results for the binary classification cases (each emotion vs other two emotions) using the absolute value of the two-sample *t*-test with pooled variance estimate are presented in Fig. 6. We can see that to distinguish the neutral emotion, we need to use the covariance of signals from channel 3 (depressor anguli oris) (is associated with sadness in [51]); for positive emotion, the covariance of signals from channel 1 (levator labii superioris), and for negative emotion, the covariance of signals from channel 3 (depressor anguli oris) and channel 4 (depressor labii inferioris). Note that negative emotional stimuli were expressed stronger and allow for better separation from other (positive and neutral) emotions.

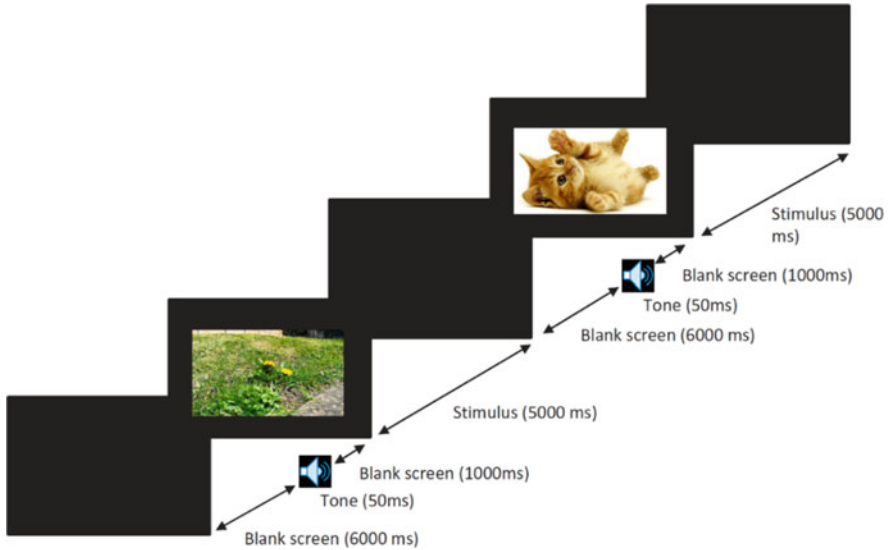


Fig. 5 Schematic diagram of the experimental protocol

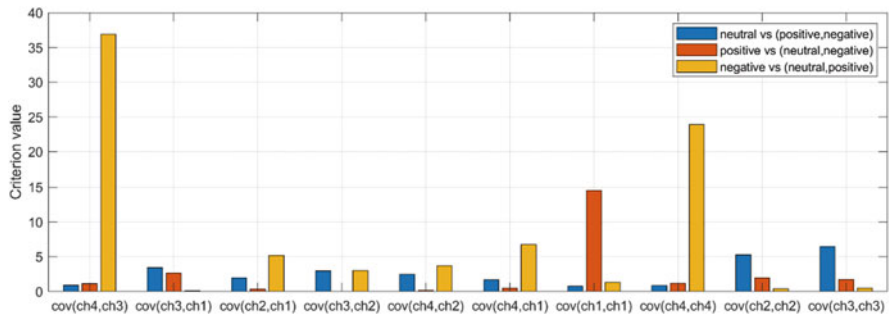
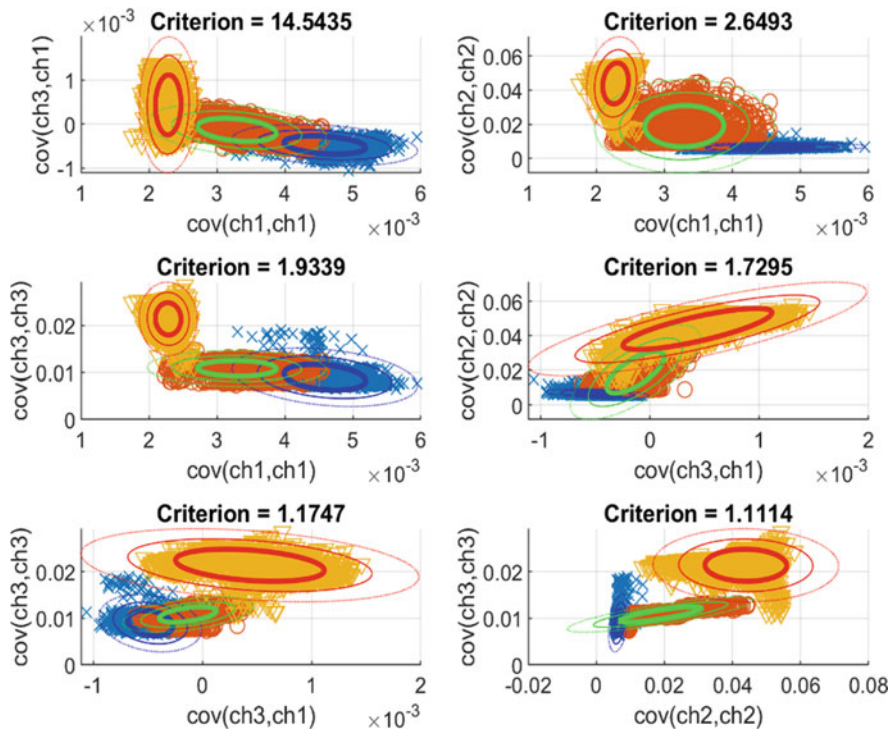


Fig. 6 Feature ranking results for binary classification of emotional responses

The distribution of clip feature values in the 2D feature space, where the feature on the x-axis corresponds to the covariance of channel 1 and the feature on the y-axis corresponds to the covariance of channels 1 and 3, is given in Fig. 7. One can see that the values corresponding to the different affective states associated with different visual stimuli (movie clips) can be separated linearly even in the 2D space but are separated even more in a higher-dimensional feature space.

The classification was performed using K-nearest neighbor (kNN) classifier. The elbow method was used to select the optimal value of the k-parameter, which was selected to be 3, in our case. One-holdout validation was adopted with 70% of data used for training step and 30% for testing step. The classification results using the kNN classifier are presented in terms of the confusion matrix shown in Fig. 8. We have achieved an accuracy of 0.976, while Kappa is 0.96 and F-score is 0.97.

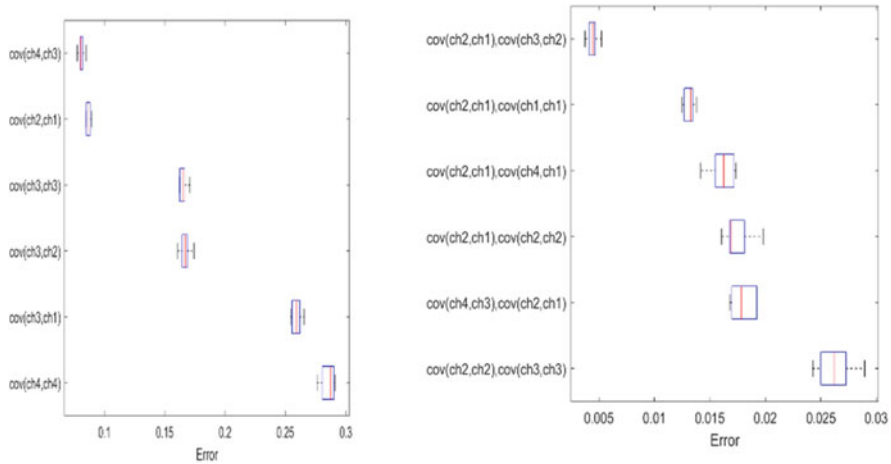


**Fig. 7** Distribution of covariance features (with 66%, 90%, and 95% confidence ellipses)

**Fig. 8** Confusion matrix of classification results for neutral, positive, and negative emotions

**Accuracy: 97.62%**

		96.5% 110	0.9% 1	0.9% 1
Predicted	Positive	96.5% 110	0.9% 1	0.9% 1
	Neutral	3.5% 4	97.3% 108	0.0% 0
	Negative	0.0% 0	1.8% 2	99.1% 110
		Positive	Neutral Actual	Negative



**Fig. 9** Classification error of top 6 features using two and three EMG channels

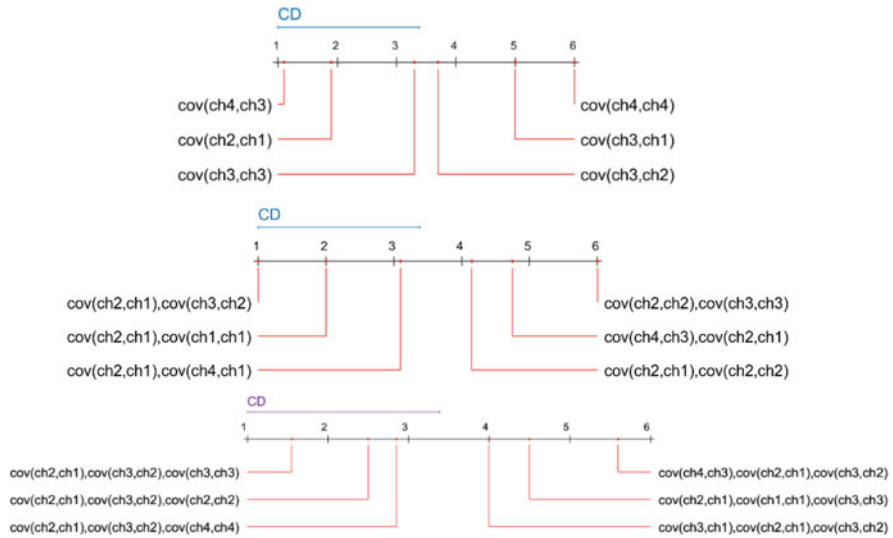
Finally, we perform the analysis of the classification results with respect to the number of features (EMG channels) used. Figure 9 shows the classification errors achieved using specific features generated from two and three EMG channels, respectively.

We performed the statistical analysis of the results using the nonparametric rank-based Friedman test and the Nemenyi post hoc test, which returns the significant differences between features. Friedman test assigns ranks to all models according to their performance. The same rank is assigned to the models if they have achieved the same performance. The null hypothesis states that there is no difference between features, and it can be accepted or rejected based on the value of Friedman test statistic. To represent the results visually, we used the critical distance diagram, in which features are sorted by their mean rank of classification accuracy along with the critical difference. Two features are significantly different if their mean rank differs by more than the critical distance (CD) (Fig. 10).

For classification using only one feature, the results of the Friedman test ( $p < 0.001$ ) show the best classification results in terms of the smallest error are achieved using the covariance of the third and fourth channel, first and second channel, and the autocovariance of the third channel (the difference between these features is smaller than critical distance, i.e., it is statistically insignificant). We can conclude that all four channels are equally important when only one feature is used for classification (see Fig. 9).

For classification using two features, the results of the rank-based Friedman test ( $p < 0.001$ ) show the best classification results in terms of the smallest error are achieved using the covariances of the first, second, and third channels and the covariances of the first, second, and fourth channels (see Fig. 9).

For classification using three features, the results of the rank-based Friedman test ( $p < 0.001$ ) show the best classification results in terms of the smallest error



**Fig. 10** Demšar significance diagram of top 6 features using two, three, and four EMG channels

are achieved using the covariances of the first, second, and third channels, but the difference with the covariances of all channels is statistically insignificant (see Fig. 9).

## 4 Conclusions

We described our experiments with the recognition of affectively induced facial expressions using on-body electromyography (EMG) sensors from the MySignals biosignal acquisition platform. For induction of the affective reaction, we used three different visual stimuli (movie clips) aimed to induce neutral, positive, and negative reactions. We have demonstrated that the facial EMG can be used as a reliable method to evaluate the affective valence of visual stimuli independent of subjective evaluation by questionnaire or verbal reports. The results from 14 subjects show that 97.6% accuracy of emotion recognition was achieved using the covariance matrix features and K-nearest neighbor (KNN) classifier. The limitations of our study are a small dataset and a small number of subjects, which we intend to solve in the future by extending the range of our experiment. The achieved results are relevant for new studies and applications in the domain of eHealth and industrial ergonomics. Future work will focus on analyzing the emotional states of office workers for smart office ergonomics, especially when facing the psychological stress of working remotely due to the COVID-19 pandemic.

## References

1. A.R. Javed, L.G. Fahad, A.A. Farhan, S. Abbas, G. Srivastava, R.M. Parizi, M.S. Khan, Automated cognitive health assessment in smart homes using machine learning. *Sustain. Cities Soc.*, 65 (2021). <https://doi.org/10.1016/j.scs.2020.102572>
2. D. Polap, G. Srivastava, K. Yu, Agent architecture of an intelligent medical system based on federated learning and blockchain technology. *J. Inf. Secur. Appl.*, 58 (2021). <https://doi.org/10.1016/j.jisa.2021.102748>
3. R.W. Picard, *Affective Computing* (MIT Press, Cambridge, MA, 1997)
4. A. Luneski, E. Konstantinidis, P.D. Bamidis, Affective medicine. *Methods Inf. Med.* **49**(3), 207–218 (2010). <https://doi.org/10.3414/me061>
5. J.M. Garcia-Garcia, V.M.R. Penichet, M.D. Lozano, J.E. Garrido, E.L.-C. Law, Multimodal affective computing to enhance the user experience of educational software applications. *Mob. Inf. Syst.*, 1–10 (2018). <https://doi.org/10.1155/2018/8751426>
6. F. Bevilacqua, H. Engström, P. Backlund, Game-calibrated and user-tailored remote detection of stress and boredom in games. *Sensors* **19**, 2877 (2019)
7. C. Filippini, E. Spadolini, D. Cardone, A. Merla, Thermal imaging based affective computing for educational robot. *Proceedings* **27**, 27 (2019)
8. G. Liaudanskaitė, G. Saulytė, J. Jakutavičius, E. Vaičiukynaitė, L. Zailskaitė-Jakštė, R. Damaševičius, Analysis of affective and gender factors in image comprehension of visual advertisement. *Adv. Intell. Syst. Comput.* **764**, 1–11 (2019)
9. P. Ekman, An argument for basic emotions. *Cognit. Emot.* **6**(3–4), 169–200 (1992)
10. P.J. Lang, The emotion probe: Studies of motivation and attention. *Am. Psychol.* **50**(5), 372 (1995)
11. I.B. Mauss, M.D. Robinson, Measures of emotion: A review. *Cognit. Emot.* **23**(2), 209–237 (2009)
12. A. Ree, I. Morrison, H. Olausson, U. Sailer, M. Heilig, L.M. Mayo, Using facial electromyography to assess facial muscle reactions to experienced and observed affective touch in humans. *J. Vis. Exp.* **145** (2019). <https://doi.org/10.3791/59228>
13. E. Coutinho, K. Gentsch, J. Van Peer, K.R. Scherer, B.W. Schuller, Evidence of emotion-antecedent appraisal checks in electroencephalography and facial electromyography. *PLoS One* **13**(1) (2018). <https://doi.org/10.1371/journal.pone.0189367>
14. A. Sahayadhas, K. Sundaraj, M. Murugappan, Detecting driver drowsiness based on sensors: A review. *Sensors* **12**(12), 16937–16953 (2012). <https://doi.org/10.3390/s121216937>
15. J. Šalkevičius, R. Damaševičius, R. Maskeliūnas, I. Laukienė, Anxiety level recognition for virtual reality therapy system using physiological signals. *Electronics* **8**, 1039 (2019)
16. J. Lee, Y. Kagamihara, S. Kakei, Quantitative evaluation of movement disorders in neurological diseases based on EMG signals. *Conf. Proc. IEEE Eng. Med. Biol. Soc.* **2008**, 181–184 (2008). <https://doi.org/10.1109/IEMBS.2008.4649120>
17. J. Wijsman, B. Grundlehner, H. Liu, J. Penders, H. Hermens, Wearable physiological sensors reflect mental stress state in office-like situations, in 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction, 2013, pp. 600–605
18. V. Raudonis, R. Maskeliūnas, K. Stankevičius, R. Damaševičius, Gender, age, colour, position and stress: How they influence attention at workplace?, in International Conference on Computational Science and Its Applications, ICCSA 2017, Trieste, Italy, July 3–6 2017, pp. 248–264. [https://doi.org/10.1007/978-3-319-62404-4\\_19](https://doi.org/10.1007/978-3-319-62404-4_19)
19. R. Maskeliūnas, T. Blažauskas, R. Damaševičius, Depression behavior detection model based on participation in serious games, in International Joint Conference on Rough Sets, IJCRS 2017, 3–7 July 2017, Olsztyn, Poland, 2017, pp. 423–434
20. S. Li, G. Walters, J. Packer, N. Scott, Using skin conductance and facial electromyography to measure emotional responses to tourism advertising. *Curr. Issue Tour.*, 1–23 (2016). <https://doi.org/10.1080/13683500.2016.1223023>





21. M. Vasiljevas, R. Turcinas, R. Damasevicius, EMG speller with adaptive stimulus rate and dictionary support. in Federated Conference on Computer Science and Information Systems, FedCSIS 2014, Warsaw, Poland, 2014, pp. 227–234. <https://doi.org/10.15439/2014F338>
22. M. Vasiljevas, R. Turčinai, R. Damaševičius (2014). Development of EMG-based speller, in ACM International Conference Proceeding Series, 10–12 September 2014
23. R. Damaševičius, M. Vasiljevas, T. Šumskas, Development of a concept-based EMG-based speller. *DYNA (Colombia)* **82**(193), 170–179 (2015)
24. K. Erin, B. Boru, Real time control of industrial robot arm with EMG and gyroscope data. *Sakarya Univ. J. Sci.*, 1 (2018). <https://doi.org/10.16984/saufenbilder.339232>
25. L. Yang, B. Kang, T. Wang, T. Zhao, An ergonomic study of Firefighters' postural comfort evaluation based on EMG method. *Adv. Intell. Syst. Comput.* **58**(1), 2310–2314 (2014)
26. V. Balasubramanian, G.S. Prasad, An EMG-based ergonomic evaluation of manual bar bending. *Int. J. Ind. Syst. Eng.* **2**(3), 299 (2007)
27. K.R. Balasubramanian, Fatigue evaluation in manual handling using surface EMG and ergonomic Design of Trolley. *Ergon. Int. J.* **2**(3) (2018)
28. M. Motamedzade, D. Afshari, A. Soltanian, The impact of ergonomically designed workstations on shoulder EMG activity during carpet weaving. *Health Promot. Perspect.* **4**(2), 144–150 (2014). <https://doi.org/10.5681/hpp.2014.019>
29. J. Kaiser, M.M. Crespo-Llado, C. Turati, E. Geangu, The development of spontaneous facial responses to others' emotions in infancy: An EMG study. *Sci. Rep.* **7**(1) (2017). <https://doi.org/10.1038/s41598-017-17556-y>
30. M. Perusqua-Hernandez, M. Hirokawa, K. Suzuki, A wearable device for fast and subtle spontaneous smile recognition. *IEEE Trans. Affect. Comput.* **8**(4), 522–533
31. M. Riehle, T.M. Lincoln, Social consequences of subclinical negative symptoms: An EMG study of facial expressions within a social interaction. *J. Behav. Ther. Exp. Psychiatry* **55**, 90–98 (2017). <https://doi.org/10.1016/j.jbtep.2017.01.003>
32. Guendil, Z., Lachiri, Z., Maaoui, C., Pruski, A. (2016). Emotion recognition from physiological signals using fusion of wavelet based features, in Proceedings of 7th International Conference on Modelling, Identification and Control, ICMIC 2015, <https://doi.org/10.1109/ICMIC.2015.7409485>
33. U. Hess, R. Arslan, H. Mauersberger, C. Blaison, M. Dufner, J.J.A. Denissen, M. Ziegler, Reliability of surface facial electromyography. *Psychophysiology* **54**(1), 12–23 (2017)
34. M.D. Latham, N. Cook, J.G. Simmons, M.L. Byrne, J.W.L. Kettle, O. Schwartz, N.B. Allen, Physiological correlates of emotional reactivity and regulation in early adolescents. *Biol. Psychol.* (2017). <https://doi.org/10.1016/j.biopsycho.2017.07.018>
35. M.S. Perez-Rosero, B. Rezaei, M. Akcakaya, S. Ostadabbas Decoding emotional experiences through physiological signal processing, in Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2017, New Orleans, LA, USA, March 5–9, 2017, pp. 881–885. <https://doi.org/10.1109/ICASSP.2017.7952282>
36. D. Thompson, I.G. Mackenzie, H. Leuthold, R. Filik, Emotional responses to irony and emoticons in written language: Evidence from EDA and facial EMG. *Psychophysiology* **53**(7), 1054–1062 (2016). <https://doi.org/10.1111/psyp.12642>
37. V. Kehri, R. Ingle, S. Patil, R.N. Awale, Analysis of facial EMG signal for emotion recognition using wavelet packet transform and SVM, in *Advances in Intelligent Systems and Computing*, (Springer, Singapore, 2019), pp. 247–257
38. S. Orguc, H.S. Khurana, K.M. Stankovic, H.S. Leel, A.P. Chandrakasan, EMG-based real time facial gesture recognition for stress monitoring, in Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2018, pp. 2651–2654
39. M.M.P. Lajante, O. Droulers, D. Amarantini, How reliable are “state-of-the-art” facial EMG processing methods?: Guidelines for improving the assessment of emotional valence in advertising research. *J. Advert. Res.* **57**(1), 28–37 (2017)
40. Y. Guo, Y. Xia, J. Wang, H. Yu, R.-C. Chen, Real-time facial affective computing on Mobile devices. *Sensors* **20**, 870 (2020)

41. M. Gazzoni, B. Afsharipour, R. Merletti, Surface EMG in ergonomics and occupational medicine, in *Surface Electromyography?: Physiology, Engineering, and Applications*, (Wiley, London, 2016), pp. 361–391
42. J. Perdiz, G. Pires, U.J. Nunes, Emotional state detection based on EMG and EOG biosignals: A short survey, in 5th Portuguese Meeting on Bioengineering, ENBENG 2017, 16–18 February 2017, Coimbra, Portugal, <https://doi.org/10.1109/ENBENG.2017.7889451>
43. A.B. Jani, R. Bagree, A.K. Roy, Design of a low-power, low-cost ECG EMG sensor for wearable biometric and medical application. 2017 IEEE Sensors, 2017, <https://doi.org/10.1109/icsens.2017.8234427>
44. M. Jiang, T.N. Gia, A. Anzanpour, A.-M. Rahmani, T. Westerlund, S. Salantera, P. Liljeberg, H. Tenhunen, IoT-based remote facial expression monitoring system with sEMG signal, in 2016 IEEE Sensors Applications Symposium (SAS), 2016
45. E. De Buyser, E. De ConinckE., B. Dhoedt, P. Simoens, Exploring the potential of combining smart glasses and consumer-grade EEG/EMG headsets for controlling IoT appliances in the smart home, in 2nd IET International Conference on Technologies for Active and Assisted Living (TechAAL 2016), 2016, <https://doi.org/10.1049/ic.2016.0053>
46. R. Rastogi, D.K. Chaturvedi, S. Satya, N. Arora, M. Gupta, V. Yadav, S. Chauhan, P. Sharma, Chronic TTH analysis by EMG and GSR biofeedback on various modes and various medical symptoms using IoT, in *Big Data Analytics for Intelligent Healthcare Management*, (Elsevier, 2019), pp. 87–150. <https://doi.org/10.1016/b978-0-12-818146-1.00005-2>
47. M. Zanghieri, S. Benatti, A. Burrello, V. Kartsch, F. Conti, L. Benini, Robust real-time embedded EMG recognition framework using temporal convolutional networks on a multicore IoT processor. *IEEE Trans. Biomed. Circuits Syst.* **14**(2), 244–256 (2020). <https://doi.org/10.1109/tbcas.2019.2959160>
48. M. Ali, A.A. Ali, A.-E. Taha, I.B. Dhaou, T.N. Gia, Intelligent autonomous elderly patient home monitoring system, in ICC 2019–2019 IEEE International Conference on Communications (ICC). ICC, 2019. <https://doi.org/10.1109/icc.2019.8761204>
49. Libelium MySignals. <http://www.my-signals.com/>. Accessed: 2/2/2021
50. E. Lopez-Larraz, O.M. Mozos, J.M. Antelis, J. Minguez, Syllable-based speech recognition using EMG, in 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, 2010, pp. 4699–4702. <https://doi.org/10.1109/IEMBS.2010.5626426>
51. van Boxtel A., Facial EMG as a tool for inferring affective states, in Proceedings of measuring behavior (Noldus Information Technology, Wageningen, 2010), pp. 104–108
52. R. Damasevicius, M. Vasiljevas, I. Martisius, V. Jusas, D. Birvinskas, M. Wozniak, BoostEMD: An extension of EMD method and its application for denoising of EMG signals. *Elektronika ir Elektrotechnika* **21**(6), 57–61 (2015). <https://doi.org/10.5755/j01.eee.21.6.13763>
53. N.E. Huang, Z. Shen, S.R. Long, M.C. Wu, H.H. Shih, Q. Zheng, H.H. Liu, The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. *Proc R Soc Lond A Math Phys Eng Sci* **454**(1971), 903–995 (1998). <https://doi.org/10.1098/rspa.1998.0193>
54. M.W. Fagerland, S. Lydersen, P. Laake, The McNemar test for binary matched-pairs data: Mid-p and asymptotic are better than exact conditional. *BMC Med. Res. Methodol.* **13**, 91 (2013). <https://doi.org/10.1186/1471-2288-13-91>
55. P. Barros, N. Churamani, E. Lakomkin, H. Siqueira, A. Sutherland, S. Wermter, The OMG-emotion behavior dataset. arXiv preprint arXiv:1803.05434, 2018
56. K.J. Varcin, S.A. Grainger, J.L. Richmond, P.E. Bailey, J.D. Henry, A role for affectivity in rapid facial mimicry: An electromyographic study. *Soc. Neurosci.* **14**(5), 608–617 (2019). <https://doi.org/10.1080/17470919.2018.1564694>

# Application of the Internet of Things (IoT) to Fight the COVID-19 Pandemic



Roseline Oluwaseun Ogundokun , Joseph Bamidele Awotunde ,  
Emmanuel Abidemi Adeniyi , and Sanjay Misra 

## 1 Introduction

The present global COVID-19 pandemic has crossed the regional, extreme, scientific, cultural, social, and pedagogical boundaries [1, 2]. In the current pandemic circumstances, every nation around the world is grappling with a pandemic and is also searching for a genuine and lucrative approach to address the glitches that arise in diverse methods. It seems the epidemic that started in Wuhan, China, is unchecked. More than 19,687,156 people have been infected by the virus, with at least 727,435 deaths globally as of 10:33 am CEST, August 10, 2020.

The Huanan Seafood Market was linked to the outbreak. The virus belongs to the species of beta coronavirus and is associated with diseases that bring about Middle East respiratory syndrome (MERS) and severe acute respiratory syndrome (SARS) [3, 93]. The WHO was first notified on December 31, 2019, even though several cases of unidentified etiology pneumonia were identified much earlier (December 8, 2019) [4, 94] (Epidemiological and clinical characteristics of 99 cases of 2019 novel coronavirus pneumonia in Wuhan, China: a descriptive study. *The Lancet*, number 395(10223), 507–513). This delay in announcing the epidemic and failure

---

R. O. Ogundokun · E. A. Adeniyi  
Department of Computer Science, Landmark University, Omu-Aran, Nigeria  
e-mail: [ogundokun.roseline@lmu.edu.ng](mailto:ogundokun.roseline@lmu.edu.ng); [adeniyi.emmanuel@lmu.edu.ng](mailto:adeniyi.emmanuel@lmu.edu.ng)

J. B. Awotunde  
Department of Computer Science, University of Ilorin, Ilorin, Nigeria  
e-mail: [awotunde.jb@unilorin.edu.ng](mailto:awotunde.jb@unilorin.edu.ng)

S. Misra (✉)  
Department of Computer Science and Communication, Ostfild University College, Halden,  
Norway  
e-mail: [sanjay.misra@hiof.no](mailto:sanjay.misra@hiof.no)

to immediately alert foreign authorities resulted in the unrestrained transmission of the virus. The pandemic is presently the focal point of worldwide concern.

In an attempt to prevent the spread of the disease, several countries were extending the lockdown, affecting millions of people. Initially, experts raised questions about the feasibility of this initiative and cautioned that certain countries were at risk of repeating a SARS-like epidemic [2, 5]. By this time, the pandemic appears to be under control in most countries, although there is still criticism of the utilization of what others have called “draconian” steps to stifle its circulation. The globe is presently trying to monitor the exceptional virus circulation that involves the greatest sum of indispositions plus deaths. As there is no such thing as definite medical care for coronaviruses and attempts to control the circulation have yet remained unsuccessful [6, 7], there’s a crucial necessity for worldwide investigation of persons with intense COVID-19 contagion.

A unified inclusion of an automated sickness management scheme could be key to managing this virus. Scientists in physical science and engineering are trying to resolve these glitches, formulate new ideas, clarify innovative research difficulties, construct user-centered clarifications, and establish themselves, including civilians in general. The IoT-enabled healthcare system is valuable for tracking COVID-19 patients properly using an integrated system. This expertise contributes to improved patient satisfaction and lowers hospital readmission rates. The IoT is a distinct scheme of interconnected computing procedures and digital and automatic gadgets capable of transmitting records across the system without human interference at some point.

Many of those tools mentioned are labelled with their respective credential numbers or codes. IoT is presently a deep-rooted and tested expertise that incorporates numerous techniques, for instance, analytics, machine learning concept, and sensual possessions. Also, IoT in traditional day-to-day operation is recognized as the usefulness of goods or devices serving people’s real-life needs in several ways, such as home protection device, smart illumination activities, and several others that are effortlessly manageable over our everyday use of smart reciters, smartphones, etc. [8, 9].

A multitude of innovative machinery in the mode of the IoT are acquiring intensifying worldwide consideration [10] and are increasingly available for the prediction, deterrence, and curbing of emerging transmittable diseases [11]. The IoT denotes an integrated network of smart gadgets, sensors, and persons from which information can be obtained in a fresh mode and distributed over cyberspace to be investigated for directions. Advanced IoT-implemented medical care management schemes (fitness management schemes) deliver actual monitoring by using wearable health tracking tools, cloud-centered inaccessible medical care research, and artificial intelligence (AI).

These control schemes incorporate the utilization of supervised, unsupervised, and machine learning in actual period, social network, public data, and medical data. As AI and machine learning integrate with the dispersed cloud, functional blockchain, device process mechanization, and AI language identification, medical care management schemes allow patients and doctors to create a robust remote

monitoring system. Therefore, the chapter discusses the overall applications of IoT during the COVID-19. The significant applications of IoT, challenges, and opportunities of deploying the technologies during the outbreak are also presented.

The manuscript is organized as follows: Sect. 2 explains the existing advanced IoT safety and addresses the key protection criteria for healthcare systems centered on IoT. We present the fundamental communication model of our anticipated IoT-established medical care framework first in Sect. 3. At this moment, the IoT-established medical care scheme is implemented utilizing body radar schemes, containing two procedures of authentication between the smart items, the local preparation unit, and the backend server. Section 4 analyzes the security sturdiness of the anticipated systems, while Sect. 5 discusses the program execution and presentation assessment. Ultimately, in Sect. 6, we made our final observations.

## 2 Internet of Things (IoT) in Healthcare Systems

The ever-increasing evolution of digital smart objects in communication technology conveys with it a novel age of application growth for IoT-established systems. Precisely, many revolutionary categories of medical care schemes with body sensor networks (BSN) have been anticipated due to the interaction-less design as well as reliability of data collection of portable smart items, for instance, wearable devices or customized biosensors [12]. The Internet of Things (IoT) is described as a collection of identifiable objects or nodes that can interact over wired or wireless networks [13, 14]. With the introduction of supercomputers, cyberspace, and wearable computing systems, the IoT is the world's third wave of intelligence [15–18]. More than 26 billion connected devices are expected to produce \$1.9 trillion in sales by 2020, according to the Internet of Things [19–21]. Moreover, 40% of IoT-connected expertise is medically associated, greater than any added group, representing a market of \$117 billion [22–24].

IoT instruments in the medical care industry, such as radars, can be used for a variety of purposes, such as heart rate monitors, glucose control, and endoscopic pills [25, 26]. The medical sector is going to be transformed by this system of sensors, actuators, and other mobile technology devices [27, 28]. The Internet of Medical Things (IoMT) is a wired system of healthcare smart gadgets that collect information from online communications systems and then pass it on to healthcare IT systems [29–31]. Currently, 3.7 million pieces of healthcare devices are in use and are connected to and tracked by various parts of the body to inform medical decisions [32, 33].

IoMTs are critical components for wearable patient care applications, such as biosystems, regeneration automation, and incident detection, among other options [34, 35]. The Internet of Things (IoT) is at the heart of mobile healthcare services, integrating implantable/wearable nodes to collect biosignals such as electromyograms (EMG) and electrocardiograms (ECG) [36–38]. IoMTs have 24/7 access to all emergency facilities, allowing prisoners to be monitored at all times. The

IoMTs have started to emerge as a focal point for telehealth supervision to alleviate the extreme lack of services available. The Internet of Medical Things (IoMT) is a collection of medical systems and platforms that link to healthcare IT systems through Internet-based computer systems. Machine-to-machine communication is allowed by medical equipment linked by wireless fidelity (Wi-Fi), which is the IoMT's concept.

Low-cost, intelligent, lightweight, and compact medical sensor nodes have been accepted in wireless transmission and wireless sensor network (WSN) technology to perfectly place themselves on the human psyche [39]. This contributes to the creation of a wireless body area network (WBAN) to track a variety of critical chronic physical ailments over time and provide real-time updates to users and medical personnel, thereby promising to revolutionize health surveillance [39]. Wireless sensor network (WSN) applications are well-thought-out solitary major fields of study for bettering the value of existence in the computer science and healthcare application industries [40].

The speedy progress in smart item expertise has encompassed important attainments in the development of applications for distributed communication systems based on wireless sensors [41]. Various revolutionary forms of on-demand and present IoT-established applications have been built as well as implemented in daily life, capitalizing on the contactlessness and reliability of information recovery from current smart items. Core data processing requirements, such as quantity, speed, variety, and, most importantly, data accuracy, ought to be carefully well-thought-out when developing IoT-established schemes [42]. However, in as much as IoT-oriented techniques pave the way for the creation of disruptive technologies, these "opportunities" pose new risks.

### **3 Application of Internet of Things Technology in COVID-19**

IoT in transmittable disease epidemiology is an evolving area, but the omnipresent proliferation of smart technology and amplified threats of transmittable diseases conveyed via global integration and worldwide interconnectivity demand its use to anticipate, deter, and monitor the evolving COVID-19 pandemic [11, 43]. Web-based monitoring platforms and strategies for disease intelligence have recently appeared in many countries [11, 43] to promote risk management and prompt identification of outbreaks, but there is a shortage of systematic use of available technologies. IoT-implemented medical care surveillance in a worldwide healthcare system would offer local health authorities the ability to strengthen efforts to identify, control, and avoid infectious diseases [44, 45].

It can help diagnose infectious patients rapidly and forecast accurately the potential circulation of an ailment to alternative places using transit data. Essentially, an IoT-established observation network may assist to rebuild and restore the economies of the source nation after an epidemic, rather than locking up major cities, borders, and businesses. Mobile connectivity in the context of mobile health (m-health) will

as well improve the productivity of a medical care network by including multiple facilities, apps, third-party APIs, and non-health-related mobile sensors [2, 46]. Security and medical care observing operations, for instance, wearable IoT, allow safety monitoring in real time and will gain developments in global health.

Due to an utter impossibility to track these large geographical regions or communities [10, 47], such innovations may eliminate holes in monitoring current systems. Such methods were introduced in the areas of computer science and healthcare analysis but are fairly new in the area of epidemiology of transmittable diseases [48, 49]. Despite the current global scenario, IoT-established smart disease detection schemes can be a significant advancement in current pandemic response exertions.

For a great deal of technologies already in position (i.e., Android phones, wearable devices, Internet access), the function that IoT can play in reducing the circulation of the disease includes simply gathering and reviewing the already collected data. The collective responsibility of IoT and connected emerging types of machinery could influence the first detection of outbreaks and deter the circulation of COVID-19 if the data was enhanced and used. Smart IoT-based disease detection systems will include continuous communication and recording, end-to-end networking and availability, data variety and review, tracing, and warnings, including choices for inaccessible healthcare support in China and other impacted countries to diagnose and control COVID-19 outbreaks.

“Ubiquitous communication” is the most fundamental technical characteristic of the IoT. The three basic mechanisms are detailed vision, intelligent computation, and efficient transmitting [9]. The utilization of IoT in the medical industry is denoted as the Internet of Medical Things (IoMT) [50], which seeks to create a decision-oriented paradigm of big data processing, assisted by information technology, for instance, exchange of ideas, telecommunications, analysis, and medication. IoMT can as well be utilized for COVID-19 deterrence and monitoring. IoT’s medical philosophy and technologies for diagnosing and treating COVID-19 can be connected to three stages.

As described above, the occurrence of COVID-19 is increasingly growing, which imposes a tremendous burden on prevention and care. There have been several reports of infections and incidents of people transmitting the virus, spreading it to other countries, which make it more difficult to curtail and handle. There are reportedly insufficient numbers of emergency staff mobilized to help in managing the pandemic. However, the efforts of these medical teams may be greatly improved by the use of IoT technology. The IoT is a crucial part of the new IT generation. The heart of the IoT is an Internet-based network that grows and extends; the user side can be extended, thus enhancing the sharing of knowledge and contact between “people.” IoMT is the science of intelligent identification, location, monitoring, and AI services for COVID-19 patients using RFID, GPS, multiple sensing instruments, knowledge sharing, and community services. If we can delve further into its function, it will undoubtedly produce unexpected outcomes.

In the therapeutic work of stopping SARIs, RFID readers can be placed on machines, and UHF stickers can be read when a drug is injected into the system



to confirm drug distribution. This clinical program has gained valuable expertise. When a robot activates the RFID reader, it can gather all of the requisite information and amounts for all of the drugs in a cabinet, and a prescription can be sent to the appropriate medical units by specifically matching the drug information. In Danville, Pennsylvania, USA, the Geisinger Medical Center has implemented integrated RFID robotics to guarantee that a drug is reliably administered to all units in operation, with images sent immediately. RFID technology can also be used to build a medical waste management network that can monitor and regulate all COVID-19 medical waste operations, including generation, recycling, transportation, and care.

Taking care of suspicious patients is a daunting task. The explanation is that it is only possible to recognize those with fever or those that have fallen sick. The other potential virus carriers aren't isolated and are the next wave of infection. Tell them to live in their own homes or to remain in the neighborhood to minimize personal transition. The recommendations suggest self-protection by practicing good hand and mouth hygiene, keeping healthy eating habits, and avoiding direct contact with those with respiratory illness symptoms (such as coughing and sneezing).

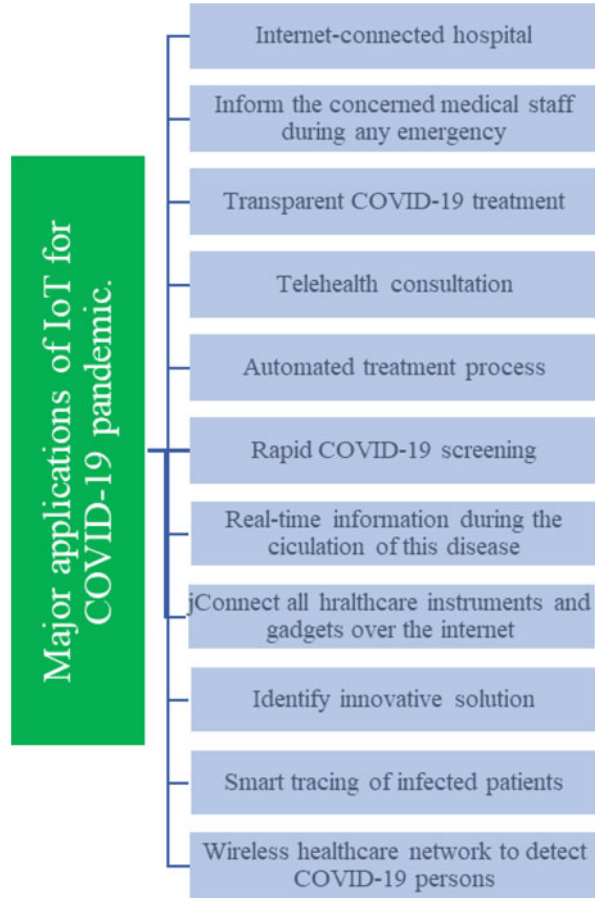
Nevertheless, the impact of this policy being followed is not understood, so there is little quality assurance. Therefore, there is an immediate need for IoT to be implemented to better handle this group of patients; compared to conventional medicine, IoMT will track the clinical and medical status of the suspicious patients during the process, illustrating the management benefits of offering customized treatment strategies for various classes of individuals. By utilizing wireless radar gadgets and modern IT, patients will benefit from medical services, thereby guaranteeing the health of suspicious patients and preventing their relatives' infection. The Internet of Medical Things (IoMT), the expanded health-specific edition of the IoT [29] applied to the present situation, should be used to build a digital forum to help people access sufficient treatment at home and to establish a robust network for policy and community organizations.

Persons with minor symptoms may receive supplies for treatment and healthcare (protective gloves, thermometers, drugs, POC COVID-19 supplies for treatment and control of infections). Inmates may upload their medical position to the IoT (medical cloud storing) portal online daily and pass their records to regional clinics, the Centers for Disease Control (CDC), or state and resident medical offices. Infirmaries might then suggest operational wellness sessions built on the medical status of each patient, and the régime (the CDC local as well as national medical offices) may perhaps distribute resources and establish isolation places (guesthouses or consolidated isolation amenities) as appropriate. This will minimize national health expenses, alleviate the pressures of medical equipment shortages, and deliver a centralized framework that would tolerate the régime to track infection transmission effectively, administer materials efficiently, and enforce response strategies. Figure 1 offered the foremost application of IoT for the COVID-19 pandemic.

The IoT is utilized for different purposes to satisfy the necessity of COVID-19 pandemic reduction results. With the aid of sufficient data collected, it has the power to forecast the coming scenario, including its solutions to handle this pandemic



**Fig. 1** Major application of IoT for the COVID-19 pandemic



properly [1]. For personalized treatment, the patient can use IoT services to properly monitor heart rate, blood pressure, and glucometer, among other things. It assists to monitor older people’s health problems as well [51, 52]. The substantial uses of this expertise in medical care are to monitor the position of healthcare gadgets and instruments for the seamless delivery of diagnosis in real time without delay. Medical care insurance providers may utilize this tool to track deception reports and deliver total scheme accountability. It increases the patient’s recovery process with effective results and also assists in decision-making during difficult situations [1].

## 4 Opportunities for Deploying the IoT Technologies During the COVID-19 Pandemic

Digital health innovations provide huge incentives to reshape current healthcare programs. Digital health innovations have offered improved quality of care at a more affordable cost, from the introduction of automated therapeutic annals to portable medical devices to other innovative technology. As part of healthcare programs, politicians are continually researching, embracing, and implementing information and communication technology (ICT) [53], which shapes how people and patients view the structures and communicate with them. The road to digital medical care (eHealth) is a systemic evolution of the conventional medical care system that incorporates numerous aspects, together with universal entry to automated medical annals, online tracking systems, inmate services, wearable devices, portable medical applications, data analytics, and further transformative innovations [53, 54]. Owing to the global COVID-19 pandemic, there is an immediate need to make good use of current technologies. The IoT is known to be one of the greatest innovative innovations with tremendous promise in combating coronavirus outbreaks [55]. The IoT consists of a sparse network where the IoT systems feel the world and transmit valuable data across the network. The IoT has been identified as one of the exciting innovations that would transform our lives due to its smooth connections and robust integration with other technologies [56]. The use of IoT in fighting this global pandemic can be expanded to many markets, each of which can play a key role in reducing the likelihood of a coronavirus pandemic [57]. Figure 2 depicts some of how IoT innovations may be useful and efficient in the fight against COVID-19.

IoMT, a subset of IoT, seeks to link patients to healthcare facilities so that vital signs can be monitored and controlled using communication infrastructure [24]. Telemedicine is becoming increasingly common in rural areas where access to a qualified physician is scarce for a variety of reasons [58]. Without patients being physically present, measurements of heart rate, electrocardiography, asthma, and vital body signs, for example, can be monitored remotely. Sensors and actuators, for example, can be used to receive data from a patient and transfer it to the cloud through a local gateway. The doctor reviews the results using either a smartphone or laptop device that has been given to them and then informs the patient or medical team who is caring for the patient about the result [59].

During the COVID-19 pandemic, digital telehealth plays a critical role. Patients can communicate with physicians via a portal, and care can be delivered online. The advantage of using a stable IoMT device during the COVID-19 pandemic is that doctors are not in close contact with the patients, preventing the virus from spreading [58]. In this moment of turmoil, several countries have begun using digital telehealth. HealthArc [60] provides patients with IoT-based healthcare equipment whose data is constantly tracked by medical personnel. The data is processed, and patients receive recommendations and prescriptions from their cell phones or tablets. Among the leading telehealth service providers are ContinuousCare [61] and Health Net Link [62]. An individual with COVID-19 symptoms should use a



Fig. 2 Prospective applications of IoT to combat COVID-19

digital platform evaluation tool, such as the “COVID-19 Gov PK mobile app” [63], which is accessible by doctors remotely. Patients are guided promptly using this instrument, and many lives will be saved. It also helps to minimize the number of hospitalizations, readmissions, and patients in hospitals, all of which contribute to improving COVID-19 patients’ quality of life and ensuring prompt care.

Ambulance medical personnel are often confronted with high-pressure, error-prone conditions [64]. During the latest COVID-19 pandemic, the situation for medical personnel coping with COVID-19 patients has become even more tense and stressful. IoT-based ambulances have an efficient approach, in which remote medical consultants advise the medical team working with the patient in the ambulance about what steps they can take. As a result, the patient receives prompt attention and is effectively managed. The equipment that uses radio-frequency identification (RFID) is connected to a wireless local area network (WLAN). The concerned medical staff has remote access to the patient’s records.

IoMT-aided equipment is classified into personal and clinical [65]. These devices keep track of the user's pulse, exercise, sleep, diet, and weight. These are also beneficial in the battle against COVID-19, as rest and sleep become very critical considerations for patients with this disease. Sleeping well boosts the body's immune system's ability to combat the virus [66]. On the portals offered by these gadget manufacturers, the patient will view his notes and, if necessary, provide input to the relevant physicians. If such algorithms are incorporated into current computers, IoT-based wearable gadgets can help reduce the spread of the coronavirus. Wearable sensors send out real-time alerts if:

- The procedure for social distancing is broken.
- There is a COVID-19 patient in the region.
- The government's declaration of a hazard zone in the event of a coronavirus outbreak.

Many countries have installed automated human body temperature monitoring devices, which include a camera that is connected with the sensor and sends real-time data to a server. The machine also employs artificial intelligence to identify a face and compare it to a consolidated database [67]. The use of these instruments aids in the tracking of COVID-19 patients. Enabling smart technology that senses the world and generates real-time reports for law enforcement authorities enforces social distancing [68]. Sensor data is continuously stored on an online database for continuous tracking [69]. The number of toxic gases or carbon content is reported to the environmental protection agency and updated on a server that can be accessed electronically [70]. Researchers are currently working on detecting coronavirus, which can be used in the same way. IBM, Microsoft, Huawei, and Cisco are only a few of the leading smart infrastructure providers [55].

Ideally, engineers and technicians would avoid traveling and visiting warehouses, isolated locations, or busy places because they fear of being infected with the virus. Nevertheless, their physical appearance on site is needed because they can't get away with manually operating the equipment available. By using special sensors mounted in machinery and enhanced knowledge, real-world overlays, and remote expert feedback, IoT may help solve their repair problems and conduct machine operation remotely, and AI may also anticipate when machines need repair (predictive maintenance) or when they might be faced with a challenge. In this way, physical visits will be significantly decreased, helping to safeguard workers' health and welfare, thus enhancing efficiencies at the level of service of the facilities.

When supermarkets continue imposing limits on sales of goods per customer, future alternatives have also been produced by IoT and AI. Smart shelves, smart fridges, video analytics, and an end-to-end integrated supply chain will help retailers deal with planning challenges and even reduce the extreme behavior of customers due to hysteria.

A couple of years ago, a major US retail chain put IoT trackers in its trolleys to prevent daily theft. Perhaps it is time to start applying this to the store shelves of important homes, sanitizers, and everything else that is already overselling in an attempt to properly control supplies and prevent hoarding behavior. Smart

watches and fitness trackers will be readily available in the not-too-distant future, and people with chronic conditions will be able to record temperature, asthma, and heartbeat without the use of intrusive instruments. For this fact, patients will be able to opt to transmit real-time and past data to public or private hospitals anytime they feel unwell so that medical health IT departments will interact with the wearables and mobile devices of patients. In this way, the treatment of coronavirus or other diseases may be prepared even more effectively and with minimal resources expended optimally. Smart connected medical devices, such as smart home ventilators, together with video and wearables, may support patients monitoring at home, give updates to those in distress, or even alert when paramedics are required to come and move them to the hospital.

Ventilators are important in treating people who have become contaminated. The health services have not been prepared to deal with this magnitude of a pandemic, and a resulting shortage is now widespread in only the most developed hospitals. An IoT-3D printing may be a lifesaver in the face of coronavirus-induced supply shortages. An IoT-3D printer offers critical medical equipment, for example, replacement valves. This is what an Italian company called Isinnova does, taking a 3D printer to a Milan hospital and manufacturing incomplete valves to be shipped to a hospital in Brescia, Northern Italy. Touch screens have been the chosen user interface (UI) until recently: among them are tablets, computers, and even doors. Nonetheless, the fact that coronavirus is more quickly transmitted from a contaminated surface than by air has made direct contact sound risky.

Many UIs that don't need any physical contact are also usable. Voice has already triumphed over tactile user interfaces, especially through smart speakers and digital helpers. Despite people confining themselves inside the building, there will be increased interest in smart home apps and the voice apps of smart speakers. Another functionality that gains ground in smartphones is beyond speech, biometrics, and their use for eye/face identification, such as the use of facial picture identification to open phones or make payments. The largest penetration is in China, but the opportunity for the remaining part of the biosphere is enormous. Wearables, for instance, smart payment watches, and other use cases (enabled by voice or close contact) can allow us to escape physical surface contact.

IoMT is the medical care-precise variant of IoT which could be introduced to deliver remedy or cure to healthcare professionals and guarantee isolation compliance which tracks disease sources [71]. With the assistance of radars embedded in smart headsets, drones, robotics, and COVID-19 self-sampling experiments, data collection may be performed. The data obtained by these techniques would be forwarded for processing to a central cloud repository. The data created by such a system would provide medical providers and government agencies better equipment to answer the COVID-19 disaster.

With these results, care professionals will be able to offer more tailor-made electronic wellness appointments for patients. Such electronic facilities will also allow patients to seek more effective treatment while reducing their access and further spreading of the virus at the same time. Agency departments, together with resident public medical offices and the Centers for Disease Control and Prevention

(CDC), will be well prepared to distribute resources, assess quarantine needs, track outbreaks, and use this information to enforce emergency plans [71].

These technologies are now being implemented in major cities to reduce the pandemic. For example, for simultaneous tracking of COVID-19 inmates, the Shanghai Public Health Clinical Center utilizes fever monitors laterally utilizing data transfer directly to the nurse post, thus minimizing possible sensitivity to healthcare workers [72]. Similarly, a device now used for medical interviews with sensors was installed in Boston to assess the breathing degree and fever of patients. In Singapore, a contact-tracing mobile program utilizes Bluetooth wireless technologies to identify individuals who were similar to COVID-19 patients [73]. Apple and Google are working on touch monitoring and detection software that will be made available to many countries around the world, which are intended to significantly step up the recognition that warns users who have been naively near to COVID-19 inmates. IoMT won't solitarily combat the present pandemic but could also be used to deter potential outbreaks.

## **5 Challenges of Using IoT During the COVID-19 Pandemic**

The main issue in the use of the IoT in the existing COVID-19 pandemic is around the protection and safety of the collected facts, which is specific and crucial as of the angle on patient welfare. The next issue concerns the maintenance to be engaged when implementing the data link amid the gadgets and protocols concerned. When more and more embedded systems are being integrated into IoT networks, the future security danger is escalating. While the IoT increases business competitiveness and strengthens the value of living for individuals, the IoT would likewise boost future hackers, and additional cyber offenders target veneers. New research performed by [74] showed that 70% of the greatest widely deployed IoT apps comprise significant susceptibilities. IoT systems are vulnerable owing to the absence of transportation security, weak user interfaces, insufficient machine protection, and insufficient authorization. The growing computer contained on average 25 holes or the risk of putting in jeopardy the domestic system. IoT systems usually don't use methods for data encryption. Any IoT technologies help critical infrastructures and vital resources like the smart grid and the security of facilities. Many IoT apps can eventually produce massive volumes of private knowledge around family, well-being, and monetary position that firms would use for their trades. The absence of protection and confidentiality would generate opposition to corporate and individual acceptance of the IoT. Training engineers could concentrate on safety difficulties via accommodating protection machinery (e.g., interruption deterrence instruments, firewalls) toward results and permitting customers to utilize IoT safety characteristics incorporated within their gadgets. This is the case for mobile safety facilities and emergency care with autonomous vehicles; IoT systems could deliver a large array of data on the position and activities of IoT customers, health habits, and buying behaviors that will all cause foremost confidentiality matters. Protecting

confidentiality in this scenario is often counterproductive for facility providers, as IoT-created data is crucial to bettering the value of an individual's existence and lowering the prices of service providers by rationalization of processes. The IoT will probably advance people's value of life. By the 2014 TRUSTe IoTs Secrecy Survey, solitary 22% of cyberspace operators accepted that any privacy issues outweighed the advantages of smart apps [75, 76]. Though IoT persists to increase traction across smart domestic schemes and wearable apps, faith in and adoption of IoT would be contingent on consumer privacy security.

IoT novelty (e.g., supercomputers, radars, cellular devices) is evolving in a very increased novelty procedure that is significantly longer than the traditional novelty dated in consumer goods. There are also overlapping requirements, weak protection, privacy concerns, complicated exchange of information, and records of badly developed gadgets proliferating. If not prudently built, multifunctional instruments and collaborative applications will turn existences into pandemonium. A minor mistake or fault in an unconnected universe does not pull a system down; but, in a very related globe, a mistake in a single aspect of a scheme will originate chaos all over. Smart house appliances and medicinal surveillance and curbing schemes are comprised of integrated radars and contact equipment and controls. If a device is malfunctioning in a medicinal track keeping and administering the scheme, the controller may acquire an inaccurate signal, which could ascertain lethal to the inmate. It's not impossible to picture smart domestic systems, for instance, thermostats and residential power meters, falling or being targeted by hackers, causing unpredicted protection difficulties. The Internet bandwidth will become overwhelmed with proliferating computer data traffic, causing latency issues around the network. A solitary computer may have an unimportant difficulty, but the chain reactions of other linked devices may be catastrophic for the network as a whole. To avert confusion in the very associated IoT environment, companies need to constitute every attempt to decrease the sophistication of wired networks, improve the reliability and uniformity of software, and ensure users' protection and confidentiality on every computer at every moment wherever.

The new wave of digitization of patient history has brought about a model change in the medical enterprise. Concerning intricacy and diversity, the enterprise is witnessing an increase in the sheer capacity of data. Big data arises as a feasible option with the commitment to change the medical care system. A model change from reactive to aggressive medical care could be responsible for a common decrease in medical costs and ultimately result in fiscal development. Even though the medical sector is harnessing the potential of big data, as new threats and vulnerabilities increase, safety and secrecy problems are becoming progressively relevant. Privacy and computer protection should be particularly considered when concerned with monitoring in healthcare. Developers can help incorporate safety into computers, applications, and systems [77]. So far as data sharing is concerned, developers should utilize a client-server method in which the server exchanges some kind of information with consumers while maintaining some information secured by acceptable authorizations [78].



Since the emergence of these innovations, data protection has to turn out to be a growing matter primarily concerning the possibility of exploitation and manipulation of data. A new area within IT has arisen, called modern ethics [79]. This division of morals is the analysis of decent issues related to data and knowledge, procedures, and related processes and substructures, as defined as in-depth in a different place [79]. Infirmity with migration must now be prepared to exchange vital details, for instance, reports from an increasing figure of persons with high fever and individuals coming in and out of the country to the IoT network, so that they can be monitored in real time. Furthermore, all relevant equipment, particularly control servers and cloud servers with a 5G system, must be deployed to ensure quick transactions to all devices accessible by computing engines and the various end-user rates.

A more thorough review of IoT applications of security needs to be discussed, as well as a more in-depth dive at the privacy issues that its implementation carries with it. Together with web-established monitoring devices, event-built IoT detection gathers and transfers raw data from an assembly of casual outlets (bulletin stories, social network messages, Twitter interrogations) to spot incidents of possible disease dissemination more rapidly than conventional, more restrictive approaches [2, 11]. This has contributed to developments in models of transmittable diseases and pathogen detection and treatment (speedy molecular recognition of pathogens) [2, 11]. Implementing automata for this pandemic, prejudice, and secrecy are the main problems during the COVID-19 pandemic when using robots. This is important to consider the risk of executing an erroneous choice amid inmates and the preservation of large gathered data [80]. IoT is the infrastructure framework most likely to continue to handle the pandemic. Patients may use their tools to monitor their vital signs. It also tracks the health conditions facing men. More notably, it manages case counseling by tracking the position of patients. The protection of the data collected is the most critical problem in applying the IoT since the data vary from a single inmate to another person [1].

Getting a smart city will be of great benefit in the fight against this pandemic by cooperation between medical centers, towns, etc. [81]. Implementing IoT-authorized smart metropolitan is one of the greatest critical sensitive solutions to the emerging pandemic. In addition to the IoT applications discussed above, [82] highlights the significance of the smart metropolitan system concept even though the globe is battling with the COVID-19 pandemic. The gathering of data from intelligent radars in IoT systems and the deployment of AIs deployed in diverse locations (generally airports and markets) will assist to counter the present and forthcoming epidemic. Database distribution and procedure standardization will contribute to safety and confidentiality problems that are required to be analyzed using correct protocols [83]. Concisely, the greater smart metropolitan infrastructure adopts interactions, the more easily the planet can cope with these pandemics [82]. Smart city technology will also allow residents to preserve social isolation by introducing innovations for transport networks, like crowd control, smart parking, and traffic displacement [68].

While data protection is still a major problem for extending these apps, healthcare providers are expected to invest \$20 billion yearly on wearable IoT systems to track



extra inmates by 2023 [83]. In Russia, a compulsory monitoring program termed social monitoring [84] was created by the régime to monitor inmates infected with COVID-19 who have to be segregated inside the geofencing features in their homes. Authorities can trace the patient after having enabled the application. Therefore, people have to apply for a quick response (QR) cipher any period they decide to migrate from the abode and report it to the police. Security issues are also correlated with government access to all this information [85, 86].

Privacy issues because the régime has entree to every statistic that is utilized to track during the pandemic is a critical question. After all, it will be known what should be achieved with the data gathered from people after the pandemic is over [87]. Since privacy is the most critical thing for deploying IoT systems to collect people's data, it could be appropriate for individuals to enable officials to access their information, despite being compensated by governments. Certain future work on the use of IoT apps may be done to provide reliable information and avoid false news. In a pandemic, they lead to tension for the population. Concerning the quarantine process, the solitary of the main issues with personal isolation is that the breathing degree will rapidly worsen. Certain portable tools introduced for this purpose can be used.

For instance, strain gauge sensor chest bands [88, 89] and moisture sensor-operating facial masks [90] and portable patchwork [91] with strain sensors may be allocated for quarantine breathing track. The reliability of this system varies between the connected users, but it still has its privacy concerns due to unstructured data collected from various users. A part of smart city, for example, touchless mobile home systems, will protect people from being contaminated throughout this pandemic. The smart metropolitan definition may remain a fantastic weapon in fighting COVID-19. IoT radars and gadgets generate huge volumes of data needed for processing and storage. The data center's present architecture is unprepared to approach the heterogeneous type and absolute volume of personal and company data [20]. Few organizations could capitalize enough in data storage to store every IoT data obtained from their networks. We should then classify data depending on needs and interests for the processes or backup. If IoT applications become more commonly used and use more bandwidth, the data centers should become more centralized to increase computing capacity and response time.

The use of data mining techniques is a must, as additional data becomes obtainable for transformation and examination. The data comprises not solitary of outdated, distinct data but likewise created continuous data by digital radars in manufacturing accessories, automobiles, automatic meters, and freighting packages. Such continuous data include setting, acceleration, sound, fever, moisture, and chemical variations in the environment as well. Data mining software may evoke disciplinary procedures to resolve urgent operating problems or warn managers about findings of competitive steps by rivals and shifts in consumer tastes that will affect their market practices in the short and long term. Computer and scientific representations need to be employed to tame and understand data. The conventional approaches of data mining do not extend specifically to unstructured images and video files. There's a lack of qualified data predictors, along with

the requirements for specialized data mining software for excavation streaming data from the radar scheme of connections as well as image and video data. The McKinsey Global Institute estimated that the United States needed 140,000–190,000 additional examining-skilled employees and 1.5 M examining-skilled executives and specialists to decide business decisions built on big data analysis [92].

## 6 Conclusion and Future Research Direction

COVID-19 is characterized by a long incubation time, high infectivity, and diagnosis difficulties, which has resulted in a sudden outbreak and widespread circulation. This situation involves IoT and big data technologies to allow swift responses and analyses, a fast provision of information about the disease environment, and an understanding of the laws of disease growth to provide timely guidance for decisions and interventions in prevention and management. IoT establishes a robust interconnected healthcare network to tackle the COVID-19 pandemic. Every healthcare gadget is associated with cyberspace, and it robotically transmits communication to the therapeutic staff during any critical situation. Infected cases with well-connected teledevices could be handled suitably in an inaccessible setting. This treats all cases smartly to provide the customer and healthcare with eventually improved support. IoT appears to be a perfect way to track the patient who is compromised. Since IoT is only a new creation, research on the psychological, behavioral, monetary, and organizational facades of IoT remains insufficient. This compels captivating knowledgeable choices concerning IoT acceptance/execution much disputing for establishments. Through utilizing a statistical-built technique, IoT becomes obliging in predicting this disease's upcoming situation. Using this technology properly applied, researchers, physicians, the community, and educators will create a safer atmosphere for battling this illness. To minimize illness and death and prevent worldwide dissemination, extra effort is required to establish automatic and efficient warning schemes to ensure immediate and appropriate identification of outbursts of these sicknesses. Such rapid and successful public health steps were engaged to reduce the likelihood of repeated epidemics and the likelihood of a resident epidemic transforming into a worldwide pandemic of COVID-19.

## References

1. R.P. Singh, M. Javaid, A. Haleem, R. Suman, Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **14**(4), 521–524 (2020)
2. M.S. Rahman, N.C. Peeri, N. Shrestha, R. Zaki, U. Haque, S.H. Ab Hamid, Defending against the novel coronavirus (COVID-19) outbreak: How can the internet of things (IoT) help to save the world. *Health Policy Technol.* **9**(2), 136–138 (2020)

3. S.Y. Fung, K.S. Yuen, Z.W. Ye, C.P. Chan, D.Y. Jin, A tug-of-war between severe acute respiratory syndrome coronavirus 2 and host antiviral defense: Lessons from other pathogenic viruses. *Emerg. Microbes Infect.* **9**(1), 558–570 (2020)
4. B. Tang, X. Wang, Q. Li, N.L. Bragazzi, S. Tang, Y. Xiao, J. Wu, Estimation of the transmission risk of the 2019-nCoV and its implication for public health interventions. *J. Clin. Med.* **9**(2), 462 (2020)
5. Z. Allam, D.S. Jones, Pandemic stricken cities on lockdown. Where are our planning and design professionals [now, then, and into the future]? *Land Use Policy* **97**, 104805 (2020)
6. G. Pullano, F. Pinotti, E. Valdano, P.Y. Boëlle, C. Poletto, V. Colizza, Novel coronavirus (2019-nCoV) early-stage importation risk to Europe, January 2020. *Eur. Secur.* **25**(4), 2000057 (2020)
7. S. Zhao, Q. Lin, J. Ran, S.S. Musa, G. Yang, W. Wang, et al., Preliminary estimation of the basic reproduction number of novel coronavirus (2019-nCoV) in China, from 2019 to 2020: A data-driven analysis in the early phase of the outbreak. *Int. J. Infect. Dis.* **92**, 214–217 (2020)
8. A. Haleem, M. Javaid, I.H. Khan, Internet of things (IoT) applications in orthopaedics. *J. Clin. Orthopaedics Trauma* **11**, S105–S106 (2020)
9. L. Bai, D. Yang, X. Wang, L. Tong, X. Zhu, N. Zhong, et al., Chinese experts’ consensus on the Internet of Things-aided diagnosis and treatment of coronavirus disease 2019 (COVID-19). *Clin. eHealth* **3**, 7–15 (2020)
10. J. Wan, M.A. Al-aqlaqi, M. Li, M. O’Grady, X. Gu, J. Wang, N. Cao, Wearable IoT enabled real-time health monitoring system. *EURASIP J. Wirel. Commun. Netw.* **2018**(1), 298 (2018)
11. E. Christaki, New technologies in predicting, preventing, and controlling emerging infectious diseases. *Virulence* **6**(6), 558–565 (2015)
12. E.A. Adeniyi, R.O. Ogundokun, J.B. Awotunde, IoMT-based wearable body sensors network healthcare monitoring system. *Stud. Comput. Intell.* **2021**(933), 103–121 (2021)
13. C. Thangavel, P. Sudhaman, Security challenges in the IoT paradigm for Enterprise information systems, in *Connected Environments for the Internet of Things*, (Springer, Cham, 2017), pp. 3–17
14. D. Bastos, M. Shackleton, F. El-Moussa, *Internet of things: A survey of technologies and security risks in smart home and city environments* (IET Conference Publications, 2018)
15. G. Shen, B. Liu, Research on application of internet of things in electronic commerce, in *2010 Third International Symposium on Electronic Commerce and Security*, (IEEE, 2010, July), pp. 13–16
16. M. Wollschlaeger, T. Sauter, J. Jasperneite, The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Ind. Electron. Mag.* **11**(1), 17–27 (2017)
17. M. Chen, Y. Miao, I. Humar, Background introduction of the internet of things, in *OPNET IoT Simulation*, (Springer, Singapore, 2019), pp. 1–76
18. M. Devarajan, L. Ravi, Intelligent cyber-physical system for an efficient detection of Parkinson disease using fog computing. *Multimed. Tools Appl.* **78**(23), 32695–32719 (2019)
19. B. Radenkovic, P. Kocovic, From ubiquitous computing to the internet of things, in *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications*, (IGI Global, 2020), pp. 1523–1556
20. J.R. Gartner, Gartner says the Internet of Things installed base will grow to 26 billion units by 2020 (2013)
21. S. Earley, Analytics, machine learning, and the internet of things. *IT Professional* **17**(1), 10–13 (2015)
22. M. Maksimović, V. Vujović, Internet of things based e-health systems: Ideas, expectations, and concerns, in *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, (Springer, Cham, 2017), pp. 241–280
23. Y. Bhatt, C. Bhatt, Internet of things in healthcare, in *The Internet of Things and Big Data Technologies for Next-Generation HealthCare*, (Springer, Cham, 2017), pp. 13–33

24. J.J. Rodrigues, D.B.D.R. Segundo, H.A. Junqueira, M.H. Sabino, R.M. Prince, J. Al-Muhtadi, V.H.C. De Albuquerque, Enabling technologies for the internet of health things. *IEEE Access* **6**, 13129–13141 (2018)
25. M. Al Ameen, J. Liu, K. Kwak, Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.* **36**(1), 93–101 (2012)
26. P.K.D. Pramanik, B.K. Upadhyaya, S. Pal, T. Pal, Internet of things, smart sensors, and pervasive systems: Enabling connected and pervasive healthcare, in *Healthcare Data Analytics and Management*, (Academic, 2019), pp. 1–58
27. S. Kumar, W. Nilsen, M. Pavel, M. Srivastava, Mobile health: Revolutionizing healthcare through transdisciplinary research. *Computer* **46**(1), 28–35 (2012)
28. A. Darwish, G. Ismail Sayed, A. Ella Hassanien, The impact of implantable sensors in biomedical technology on the future of healthcare systems, in *Intelligent Pervasive Computing Systems for Smarter Healthcare*, (Wiley, 2019), pp. 67–89
29. G.J. Joyia, R.M. Liaqat, A. Farooq, S. Rehman, Internet of medical things (IOMT): Applications, benefits and future challenges in the healthcare domain. *J. Commun.* **12**(4), 240–247 (2017)
30. G. Manogaran, N. Chilamkurti, C.H. Hsu, Emerging trends, issues, and challenges on the Internet of Medical Things and wireless networks. *Pers. Ubiquit. Comput.* **22**(5–6), 879–882 (2018)
31. B. Marr, Why the internet of medical things (iomt) will start to transform healthcare in 2018 (2018)
32. U. Varshney, *Pervasive Healthcare Computing: EMR/EHR, Wireless and Health Monitoring* (Springer Science & Business Media, 2009)
33. Y.A. Qadri, A. Nauman, Y.B. Zikria, A.V. Vasilakos, S.W. Kim, The future of healthcare internet of things: A survey of emerging technologies. *IEEE Commun. Surv. Tutorials* **22**(2), 1121–1167 (2020)
34. S. Pirbhulal, W. Wu, G. Li, A biometric security model for wearable healthcare, in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, (IEEE, 2018, November), pp. 136–143
35. A. Mavrogiorgou, A. Kiourtis, M. Touloupou, E. Kapassa, D. Kyriazis, Internet of medical things (IoMT): Acquiring and transforming data into HL7 FHIR through 5G network slicing. *Emerg. Sci. J.* **3**(2), 64–77 (2019)
36. N. Zhang, J. Zhang, H. Li, O.O. Mumini, O.W. Samuel, K. Ivanov, L. Wang, A novel technique for fetal ECG extraction using a single-channel abdominal recording. *Sensors* **17**(3), 457 (2017)
37. H. Magsi, A.H. Sodhro, F.A. Chachar, S.A.K. Abro, G.H. Sodhro, S. Pirbhulal, Evolution of 5G on internet of medical things, in *2018 International Conference on Computing, Mathematics, and Engineering Technologies (iCoMET)*, (IEEE, 2018, March), pp. 1–7
38. A.H. Sodhro, A.K. Sangaiah, S. Pirphulal, A. Sekhari, Y. Ouzrout, Green media-aware medical IoT system. *Multimed. Tools Appl.* **78**(3), 3045–3064 (2019)
39. L. Hughes, X. Wang, T. Chen, A review of protocol implementations and energy efficient cross-layer design for wireless body area networks. *Sensors* **12**(11), 14730–14773 (2012)
40. A. Darwish, A.E. Hassanien, Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors* **11**(6), 5561–5595 (2011)
41. S.E. Bibri, The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustain. Cities Soc.* **38**, 230–253 (2018)
42. E. Ahmed, I. Yaqoob, I.A.T. Hashem, I. Khan, A.I.A. Ahmed, M. Imran, A.V. Vasilakos, The role of big data analytics in the Internet of Things. *Comput. Netw.* **129**, 459–471 (2017)
43. S.K. Udgata, N.K. Suryadevara, COVID-19: Challenges and advisory, in *The Internet of Things and Sensor Network for COVID-19*, (Springer, Singapore, 2020), pp. 1–17
44. M.M. Alam, H. Malik, M.I. Khan, T. Pardy, A. Kuusik, Y. Le Moullec, A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **6**, 36611–36631 (2018)

45. H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, M. Alizadeh, *The Application of the Internet of Things in Healthcare: A Systematic Literature Review and Classification* (Universal Access in the Information Society, 2019), pp. 1–33
46. S. Nazir, Y. Ali, N. Ullah, I. García-Magariño, Internet of things for healthcare using effects of mobile computing: A systematic literature review. *Wirel. Commun. Mob. Comput.* **2019**, 1–20 (2019)
47. F. Wu, T. Wu, M.R. Yuce, An internet-of-things (IoT) network system for connected safety and health monitoring applications. *Sensors* **19**(1), 21 (2019)
48. T.A. Hammad, M.F. Abdel-Wahab, N. DeClariss, A. El-Sahly, N. El-Kady, G.T. Strickland, Comparative evaluation of the use of artificial neural networks for modeling the epidemiology of schistosomiasis mansoni. *Trans. R. Soc. Trop. Med. Hyg.* **90**(4), 372–376 (1996)
49. S. Ogino, R. Nishihara, T.J. VanderWeele, M. Wang, A. Nishi, P. Lochhead, et al., The role of molecular pathological epidemiology in the study of neoplastic and non-neoplastic diseases in the era of precision medicine. *Epidemiology (Cambridge, MA)* **27**(4), 602 (2016)
50. Y. Song, J. Jiang, X. Wang, D. Yang, C. Bai, Prospect and application of Internet of Things technology for prevention of SARIs. *Clin. eHealth* **3**, 1–4 (2020)
51. M. Shahidul Islam, M.T. Islam, A.F. Almutairi, G.K. Beng, N. Misran, N. Amin, Monitoring of the human body signal through the Internet of Things (IoT) based LoRa wireless network system. *Appl. Sci.* **9**(9), 1884 (2019)
52. G. Marques, R. Pitarma, M. Garcia, N. Pombo, Internet of Things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: A review. *Electronics* **8**(10), 1081 (2019)
53. P.P. Sust, O. Solans, J.C. Fajardo, M.M. Peralta, P. Rodenas, J. Gabaldà, et al., Turning the crisis into an opportunity: Digital health strategies deployed during the COVID-19 outbreak. *JMIR Public Health Surveill.* **6**(2), e19106 (2020)
54. B. Meskó, Z. Drobni, É. Bényei, B. Gergely, Z. Györfy, Digital health is a cultural transformation of traditional healthcare. *Mhealth* **3**, 38 (2017)
55. M. Kamal, A. Aljohani, E. Alanazi, IoT meets COVID-19: Status, challenges, and opportunities. *arXiv preprint arXiv, 2007.12268* (2020)
56. F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutorials* **22**(3), 1686–1721 (2020)
57. N. Saeed, A. Bader, T.Y. Al-Naffouri, M.S. Alouini, When wireless communication faces COVID-19: Combating the pandemic and saving the economy. *arXiv preprint arXiv, 2005.06637* (2020)
58. S.C.I. Chen, R. Hu, R. McAdam, Smart, remote, and targeted health care facilitation through connected health: Qualitative study. *J. Med. Internet Res.* **22**(4), e14201 (2020)
59. A. Poppas, J.S. Rumsfeld, J.D. Wessler, Telehealth is having a moment: Will it last? *J. Am. Coll. Cardiol.* **75**(23), 2989–2991 (2020)
60. G.A. Olsen U.S. Patent Application No. 15/339,639 (2017)
61. R. Crowley, H. Daniel, T.G. Cooney, L.S. Engel, Envisioning a better US health care system for all: Coverage and cost of care. *Ann. Intern. Med.* **172**(2\_Supplement), S7–S32 (2020)
62. HealthnetConnect. Healthcare delivery, reimaged. <https://healthnetconnect.com/>. Accessed on 6/08/2020
63. R. Ohannessian, T.A. Duong, A. Odone, Global telemedicine implementation and integration within health systems to fight the COVID-19 pandemic: A call to action. *JMIR Public Health Surveill.* **6**(2), e18810 (2020)
64. E. Park, J.H. Kim, H.S. Nam, H.J. Chang, Requirement analysis and implementation of smart emergency medical services. *IEEE Access* **6**, 42022–42029 (2018)
65. H. Habibzadeh, K. Dinesh, O.R. Shishvan, A. Boggio-Dandry, G. Sharma, T. Soyata, A survey of healthcare internet of things (HIoT): A clinical perspective. *IEEE Internet Things J.* **7**(1), 53–71 (2019)
66. Y. Bai, L. Yao, T. Wei, F. Tian, D.Y. Jin, L. Chen, M. Wang, Presumed asymptomatic carrier transmission of COVID-19. *JAMA* **323**(14), 1406–1407 (2020)

67. I.C. Konstantakopoulos, A.R. Barkan, S. He, T. Veeravalli, H. Liu, C. Spanos, A deep learning and gamification approach to improving human-building interaction and energy efficiency in smart infrastructure. *Appl. Energy* **237**, 810–821 (2019)
68. M. Gupta, M. Abdelsalam, S. Mittal, Enabling and enforcing social distancing measures using smart city and its infrastructures: A COVID-19 use case. arXiv preprint arXiv, 2004.09246 (2020)
69. R. Mehmood, S.S.I. Katib, I. Chlamtac, *Smart Infrastructure and Applications* (Springer International Publishing, 2020)
70. S.L. Ullo, G.R. Sinha, Advances in smart environment monitoring systems using IoT and sensors. *Sensors* **20**(11), 3113 (2020)
71. T. Yang, M. Gentile, C.F. Shen, C.M. Cheng, Combining point-of-care diagnostics and the internet of medical things (IoMT) to combat the COVID-19 pandemic. *Diagnostics* **10**(4), 224 (2020)
72. D. Koh, SPHCC employs IoT tech and wearable sensors to monitor COVID-19 patients. *Mobi Health News*. <https://www.mobihealthnews.com/news/asia-pacific/sphcc-employs-iot-tech-and-wearable-sensors-monitor-covid-19-patients>. Accessed 04 Apr 2020 (2020)
73. H. Baharudin, L. Wong, *Coronavirus: Singapore Develops a Smartphone App for Efficient Contact Tracing*. <https://www.straitstimes.com/singapore/coronavirus-singapore-develops-smartphone-app-for-efficient-contact-tracing>
74. Hewlett Packard, *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack* (2014, July 29)
75. M. Langheinrich, F. Schaub, Privacy in mobile and pervasive computing. *Synth. Lect. Mob. Pervasive Comput.* **10**(1), 1–139 (2018)
76. TRUSTe. *TRUSTe Internet of Things Privacy Index—US Edition*. (2014)
77. D. Kotz, K. Fu, C. Gunter, A. Rubin, Security for mobile and cloud frontiers in healthcare. *Commun. ACM* **58**(8), 21–23 (2015)
78. P. Kampanakis, Security automation and threat information-sharing options. *IEEE Secur. Privacy* **12**(5), 42–51 (2014)
79. L. Floridi, Soft ethics, the governance of the digital, and the general data protection regulation. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **376**(2133), 20180081 (2018)
80. A. Howard, J. Borenstein. *AI, Robots, and Ethics in the Age of COVID-19*. Retrieved May 18, 2020. (2020)
81. R. Djalante, R. Shaw, A. DeWit, Building resilience against biological hazards and pandemics: COVID-19 and its implications for the Sendai framework. *Prog. Disaster Sci* **6**, 100080 (2020)
82. Z. Allam, & D.S. Jones, On the coronavirus (COVID-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management, in *Healthcare*, (vol. 8, no. 1, Multidisciplinary Digital Publishing Institute, 2020, March), p. 46
83. A.A. Alyami, Smart e-health system for real-time tracking and monitoring of patients, staff, and assets for healthcare decision support in Saudi Arabia (Doctoral dissertation, Staffordshire University) (2018)
84. M. Al-Khafajiy, T. Baker, C. Chalmers, M. Asim, H. Kolivand, M. Fahim, A. Waraich, Remote health monitoring of elderly through wearable sensors. *Multimed. Tools Appl.* **78**(17), 24681–24706 (2019)
85. Küpper, A., Bareth, U., & Freese, B. Geofencing and background track—the next features in LBSs. In *Proceedings of the 41st Annual Conference of the Gesellschaft für Informatik eV* (2011).
86. M. Nasajpour, S. Pouriyeh, R.M. Parizi, M. Dorodchi, M. Valero, H.R. Arabnia, Internet of things for current COVID-19 and future pandemics: An exploratory study. arXiv preprint arXiv, 2007.11147 (2020)
87. R.K.R. Kummitha, Smart technologies for fighting pandemics: The techno-and human-driven approaches in controlling the virus transmission. *Gov. Inf. Q.* **37**, 101481 (2020)

88. L. Al-Ghussain, S. El Bouri, H. Liu, D. Zheng, Clinical evaluation of stretchable and wearable inkjet-printed strain gauge sensor for respiratory rate monitoring at different measurement locations. *J. Clin. Monit. Comput.*, **35**(3), 453–462 (2020)
89. L. Wang, K.J. Loh, Wearable carbon nanotube-based fabric sensors for monitoring human physiological performance. *Smart Mater. Struct.* **26**(5), 055018 (2017)
90. J. Dai, H. Zhao, X. Lin, S. Liu, Y. Liu, X. Liu, et al., Ultrafast response polyelectrolyte humidity sensor for respiration monitoring. *ACS Appl. Mater. Interfaces* **11**(6), 6483–6490 (2019)
91. M. Chu, T. Nguyen, V. Pandey, Y. Zhou, H.N. Pham, R. Bar-Yoseph, et al., Respiration rate and volume measurements using wearable strain sensors. *NPJ Digital Med.* **2**(1), 1–9 (2019)
92. J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (McKinsey & Company, 2011, May)
93. R.O. Ogundokun, A.F. Lukman, G.B. Kibria, J.B. Awotunde, B.B. Aladeitan, Predictive modeling of COVID-19 confirmed cases in Nigeria. *Infect. Dis. Model.* **5**, 543–548 (2020)
94. M. Daniyal, R.O. Ogundokun, K. Abid, M.D. Khan, O.E. Ogundokun, Predictive modeling of COVID-19 death cases in Pakistan. *Infect. Dis. Model.* **5**, 897–904 (2020)

# An Enhanced IoT-Based Array of Sensors for Monitoring Patients' Health



Modupe Odusami, Sanjay Misra , Olusola Abayomi-Alli, Shobayo Olamilekan, and Chukwuebuka Moses

## 1 Introduction

Health monitoring systems are becoming more critical, and the Internet of things (IoT) technology offers an effective approach to handle real-time service in health care [37, 42]. Automatic and mobile-based health monitoring devices are gaining momentum nowadays [1, 2, 20, 21, 31]. This is partly due to the shortage of the number of available doctors in the rural areas as compared to their urban counterparts. In these rural areas, medical equipment is also hard to come by, and when available, most of this equipment is already in bad condition in poorly funded government hospitals in developing countries. Hypertension has pride itself to be the root cause of cardiac/stroke mortality among many other chronic illnesses affecting humankind [24]. The advent of the Internet of Things (IoT) has led to the seamless integration of computing devices that can connect to the Internet to be able to provide the health details of a patient to a remote doctor in real time. These devices are known as IoT devices, and they can be categorized as physical assets, such as sensors, machines, gateways, and networks. They can connect people to things (people to objects) and things to things (objects to objects).

---

M. Odusami · S. Olamilekan · C. Moses

Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria  
e-mail: [olamilekan.shobayo@covenantuniversity.edu.ng](mailto:olamilekan.shobayo@covenantuniversity.edu.ng)

S. Misra (✉)

Department of Computer Science and Communication, Ostfold University College, Halden, Norway  
e-mail: [sanjay.misra@hiof.no](mailto:sanjay.misra@hiof.no)

O. Abayomi-Alli

Department of Software Engineering, Kaunas University of Technology, Kaunas, Lithuania  
e-mail: [olusola.abayomi-all@ktu.edu](mailto:olusola.abayomi-all@ktu.edu)



Typically, an IoT network can grow radically in an uncontrolled manner. This can lead to an increase in a variety of data that it processes, computational speed of the data, and size of data as well [30]. This increase in the speed and size of data that IoT devices process on a daily basis can lead to money-making opportunities and value expansion. The only shortcoming from this large chunk of data is the availability of sophisticated tools to analyze them and be able to conclude them in real time [16].

The sophisticated and complex nature of the IoT technology coupled with the frenzy created by the Internet, mobile technology, and an ever-present IT environment has created a sort of urgency to build powerful analytical tools [7]. Making the industry a very viable option requires the ability to use these data for real-time predictions. In contrast to the pre-IoT era, where, for instance, a typical supply chain challenge takes about 2–3 days to be resolved, cases nowadays take a very short time to be handled in these days of IoT, for example, time periods such as 30 min for the rectification of electrical faults to 30-s reaction times to information from devices to even a 5-millisecond reaction to breaches in security [22].

This data explosion and high expectations experienced in the IoT environment can lead to loss of value of data due to the short lifespan. Hence, there is a need to act on this data in real time. The importance of timeliness of IoT data can be experienced in a wide range of applications and use cases. These applications can be grouped into three parts: long-term growth and innovation on new products and services can increase revenue and raise the value of a business, operations and fulfillment are in the right place to provide efficiency gains, and applications are focused on sales and marketing, which will increase customer satisfaction [18].

Some other specific use cases, such as demand/supply optimization, predictive maintenance, and predictive one-on-one marking and outage management, are also available within the application. To be able to address the time required for actions to be taken on these application use cases, an advanced and sophisticated analytic solution is required, which combines real-time streaming and predictive, historical, and prescriptive analytics as well as provides top-notch analysis and smarter resolutions [8, 10, 40].

The Bluetooth technology thrives on its low battery consumption, but it also lacks in its range of connectivity [44]. The Zigbee module's downside is having a limited bandwidth of 250 kbps, which takes up to four times more time to transmit a fixed amount of data compared to other technologies. The Bluetooth technology, which allows the implementation of a single sensor, has shown to be a promising technology in the healthcare system [23]. However, this technology can be improved via the implementation of simultaneous transmission of ECG data via ADC. This speeds up the ECG sampling process and, in effect, generates complete and accurate ECG data. Also, various vital sign devices are standalone, and even those equipped with multiple sensors are either two or three. Some of the IoT-enabled health monitoring systems focused on a single parameter. One important point to consider here is how to integrate several sensors together into a single device for the health monitoring system. The main contributions of this paper are as follows:

- The design of an automatic health monitoring system using an Arduino device and a Wi-Fi module relays the information to ThingSpeak cloud-based web servers.
- To integrate different sensors, such as temperature sensor, UV sensor, pulse sensor, and heartbeat sensor, which are IoT-enabled.
- To develop an easy-to-use, cost-effective smart system that will enable patients or individuals to monitor their vital signs and enable doctors to remotely monitor patients' health via the Internet easily using IoT.

The rest of the paper is organized as follows: Sect. II covers the background of IoT sensors in health monitoring systems. Section III discusses in detail the related works with highlights on the limitations of existing approaches. Section IV presents the method used with a detailed description of the sensing units, the controlling unit, and the display unit. Section V describes the results achieved in the proposed system. The paper concludes in Sect. VI with future research and recommendations.

## 2 Background and Related Work

The Internet and its applications have become an integral part of the human lifestyle today. In every aspect, it's become an essential tool. IoT technology has completely changed the narratives of society by giving us the ability to track and manage important phenomena in our environment through devices that can sense, store, and transfer information wirelessly to remote storage, such as cloud for analysis and presentation in a human-readable form [17].

Researchers went beyond just connecting computers to the web because of the tremendous demand and necessity. These researches led to a groundbreaking gizmo, the IoT, being developed. The IoT technologies were suggested years ago, but it is still in the initial phase of commercial implementation [12]. The increased use of mobile technologies and smart devices in the healthcare sector has a major impact on the world. The eradication of diseases and illnesses requires careful monitoring of one's health. Health experts are gradually taking advantage of these innovations, thereby creating a major change in healthcare. Likewise, several people are provided with the advantages of m-Health (mobile health) and e-Health (ICT-supported healthcare) applications to improve and assist their well-being. In order to contribute to and expand the overall healthcare system, various devices and systems can work together in the scope of IoT. End-user healthcare applications need a variety of knowledge about a patient's condition and environment to better understand the health of the patient and the type of treatment required. This data is gathered from a collection of sensors with different applications [27]. The system facilitates real-time analysis of various patient vitals, such as heart rate, temperature, foot pressure, and ECG. Data emanating from the system is transferred to the cloud using an IoT device. The main function of the IoT device is to connect the various sensors to a central platform.

IoT has recently become an area of enormous concern for both risk investors and technology companies, contributing to a multitude of research and business initiatives. Smart grid, smart towns, smart wearable devices, and smart homes are some of the applications that have gained great attention. Nearly every IoT device requires some sensors and transducers usually attached to a microcontroller and a wireless link that connects to a remote cloud server or a local repository and has the capacity to turn preprocessed data into useful information. This section discusses the various studies tailored toward IoT patient health monitoring systems.

## ***2.1 Related Studies on IoT Patient Health Monitoring System***

Raiz [29] designed a system monitoring the heartbeat and blood pressure of a patient with the Arduino serving as a bridge that uploads the data collected from the sensors to the web. Low cost and efficiency were some of the authors' strengths. However, the authors did not consider enough parameters to be measured. Sivasankari et al. [33] concentrated on temperature, blood pressure measurement, and pulse rate sensor using the Arduino ATmega328P AVR microcontroller. The results gotten from the Arduino were uploaded to the LabVIEW. Medical doctors could view their patient chart data in real time, and the data gotten from the patients are stored in an excel sheet on the cloud for easy access. However, the cost of implementation was very high. Similarly, Vippalapalli and Ananthula [38] proposed a system to measure patients' vitals with heartbeat sensors, temperature sensors, eyeblink sensor, ECG sensors, and Arduino ATmega328P; the microcontroller transmits the data to a cloud-based website called ThingSpeak. Akshaya et al. [4] used the Raspberry Pi as a connecting point between the input of the sensor and the virtual network computing (VNC) server. Each of the sensors, namely, blood pressure sensor, body temperature sensor, electrical sensor, pulse/heartbeat sensor, and patient location sensor, is connected to the Raspberry Pi.

Signals of Raspberry Pi can be shown on the window, and the importance of these sensors can be shown on the doctor's local area network or Wi-Fi-compatible Raspberry Pi VNC server. Similarly, signals from temperature transducers, heartbeat sensors, and respiration are sent to the Raspberry Pi with the use of signal conditioning and an amplifier circuit according to Uddin et al. [36]. Furthermore, Rahman et al. [28] proposed a Raspberry Pi system as a central device that connects the input and output device. The data gotten from the sensors, such as ECG and the temperature sensors, are sent to the Arduino Uno, sending the data to the Raspberry Pi. One major limitation of the approach is the low signal gain, which can lead to data loss. Kumar and Rajasekaran [14] proposed a system that monitors health using Raspberry Pi and IoT. This system used measurements derived from four physiological parameters: the accelerometer sensor, the respiratory sensor, and the heartbeat sensor. The sensory units' captured signal was also amplified and conditioned before passing through to the Raspberry Pi.

The proposed system was very effective in monitoring patient's health. Future work introduces more parameters and utilizes web applications so that patient's

data can be accessed anywhere in the world. Rajkumar et al. [26] proposed a health monitoring system based on temperature and heart rate. The details of the patients' medications were stored in a local repository made available in the Raspberry Pi, and the body temperature of the patient and their heartbeat were monitored by temperature sensor and heartbeat sensor, respectively. These devices were also connected to the Raspberry Pi through Fitbit.

The temperature value was also extracted the same way. The doctors get notified via SMS, if there is an anomaly in the patients' data. The proposed system reduced healthcare costs and facilitated a faster way to detect the problem. However, patient's data are not easily accessible at all times. Furthermore, proposed Arduino Uno and Raspberry Pi's use for monitoring patient's health through the Internet. The physiological component of the human body used includes blood pressure, body temperature, oxygen level in the blood, and pulse rate. Zigbee was utilized for the transmission of data from Arduino to the Raspberry Pi. The proposed system is useful in monitoring the health status of older adults. Purnima [25] upped the ante by designing a patient monitoring system that is more reliable and energy-efficient. They were able to incorporate real-time transmission of patient's parameters, i.e., location, temperature, heartbeat, and ECG. The protocol used for transmitting the data is the Zigbee module, which is connected to an Arduino Uno. Kumar and Pandey [13] also proposed a similar health monitoring system that was able to track vital health parameters. They included a human skin response sensor and glucose level sensor in addition to the pulse rate, blood pressure, and body temperature sensors, respectively.

Zigbee IEEE 801.15.4 was used for data transmission to provide a low-cost solution. Nurdin et al. [19] used only the ECG sensor connected to the Zigbee module. The data sent to the Zigbee module is transmitted to a testing webserver called the web stress tool and apache benchmark. One of the drawbacks was that the Zigbee interface could only allow 20 users. Deepa and Kumar [6] designed a smart noninvasive wearable monitoring device using Zigbee developed and designed to measure physiological parameters, such as temperature, heart rate, blood pressure, and patients' movement. The machine contains an electronic gadget worn on a dangerous person's wrist or arm. To detect falling, an impact sensor was used. The results were obtained with the software LabVIEW. Sollu et al. [34] proposed a heart rate monitoring system and body temperature using the Raspberry Pi. The patient's data stored on the Raspberry Pi can be viewed on a personal computer. The proposed system error rate in detecting heartbeat rate and body temperature was very insignificant. Warsi et al. [39] presented a model based on IoT for remote patient health observation. Through the use of sensors, the device was capable of monitoring the essential vital elements of patients at home or remotely, such as temperature, blood pressure, heartbeat, and electrocardiographic readings. The doctor can monitor the patient's live status from anywhere from a remote location without being restricted due to Internet access to receive live patient notifications. The model introduced is highly useful to society and supports the current health monitoring solutions. Akhila et al. [3] proposed a microcontroller-based patient health monitoring system using Arduino and Atmega328 microcontroller to obtain readings from a heartbeat,

blood pressure, and body temperature transducer. ThingSpeak was used to store the transducer readings to the cloud recorded in the Arduino Uno via the Wi-Fi module. From experimental results, the proposed system showed high reliability, great returns, and user-friendliness. The shortcoming of the system is that only three vitals were taken into consideration, and improvements can be suggested, such as adding more parameters like body mass index (BMI) and body glucose level. Singh and Jain [32] performed an experiment on the performance and evaluation of Bluetooth technology-related blood pressure monitoring systems. Preliminary results obtained indicate the prototype developed can give results with some degree of confidence, and the criteria set by the Association for the Advancement of Medical Instrumentation was duly met. Further recommendations for the work are to include all other parameters to improve the robustness of the system. And also, several other technologies can be incorporated into the analysis of the design.

Tello et al. [35] proposed a remote health monitoring system that measures the body temperature and electrocardiogram (ECG). The medium for transmission is the Bluetooth module, and the data collected here is displayed on an LCD screen. The information could later be accessed through a web application platform using Internet connectivity. The performance of the proposed model was verified using 13 volunteers and could be effectively used in remote areas; optimal connectivity is not classified as an important parameter. Experimental results also showed that there was a delay in the signals received by the proposed model. Majumder et al. [15] proposed a health monitoring system that is wearable and user-friendly and continuously monitors body vitals such as heart rate, blood pressure, and body temperature. An Arduino was implemented for the data acquisition unit. The Bluetooth technology was utilized for the means of data transmission in order to achieve a cost-efficient model. The proposed system was very effective in getting different vital sign readings when the patients or doctors wish to. The implemented device was easily portable and cheaper than other devices and proven to be an appropriate solution for densely populated countries. Future work is the inclusion of ECG sensor and respiratory rate checking unit. Zainal et al. [43] presented wireless photoplethysmography data acquisition for health monitoring systems using Bluetooth technology, and the outcome was able to fulfill the desire of producing a valuable product. Li and Pan [11] proposed a health monitoring system based on IoT. The physiological parameters monitored are temperature, ECG, and pulse rate, and the measured data were transmitted through Bluetooth to the Android platform. The medical doctors were able to contact the patients through GPRS, which is connected to the mobile platform. Experimental results showed that the proposed model gave a high accuracy. Future work is the utilization of Wi-Fi technology, which is capable of greater connectivity both indoors and outdoors. Hasan and Ismaeel [9] proposed an ECG monitoring system based on Arduino Uno, ESP8266 Wi-Fi module, and Blynk IoT application. The Blynk IoT application is used by physicians to monitor the heart conditions of their patients. The proposed system is very easy to use by anyone and is cost-effective. Bharadwaj et al. [5] presented a health monitoring system using Arduino and ThingSpeak. The parameters measured were ECG and temperature. The acquired data is sent to a web

server in real time for doctors to be able to view the patients' vital signs anytime. The proposed system is very cost-effective. The authors recommended the utilization of a mobile platform to enable the use of SMS, especially when there is an emergency. Yeri and Shubhangi [41] proposed a real-time health monitoring system consisting of web and mobile applications. The major sensors used to capture patients' vital are temperature sensors, pulse sensors, and SpO2 sensors. The data acquired from the sensor devices is transmitted to the cloud via a Wi-Fi module that interfaced with Arduino Uno. The system allows doctors to monitor their patients' health remotely, and the patients via the system can seek medical care from any specialist all over the world. The system can be upgraded by incorporating another sensor that will allow regular checkups of the client.

The summary of some related works in the health monitoring system using different technologies and the number of parameters considered for patient monitoring is presented in Table 1. Some of the limitations affecting research efforts are the absence of a cloud base database, delay in signals, limited connectivity, obstruction of data transmitted, and limited sensory units. However, there is a need for effective and affordable methods that will integrate more sensors in one device for patient's health monitoring system [15].

### 3 Proposed Approach

The proposed system uses four vitals for the health monitoring system. These vitals use four sensors in return, which are heartbeat sensor, temperature sensor, UV sensor, and pulse sensor. These sensors are connected to an 8-bit ATmega328P Arduino board. ThingSpeak acts as the remote cloud-based repository that connects the doctor's computer to the Arduino Uno through the ESP8266-1 Wi-Fi module. This system's advantage is that it adds four vitals where other works have used less and integrates all the components on one device. The block diagram of the proposed system is depicted in Fig. 1.

#### 3.1 Pulse Sensor

This study uses a pulse sensor that comprises two parts: the light sensor and the circuitry on the other side. The LED is specifically located on the vein, and it flashes with each pulse. The technical specifications are as follows: 5 V operating voltage, green LED as a transmitter, and optical receiver.

#### 3.2 Heartbeat Sensor

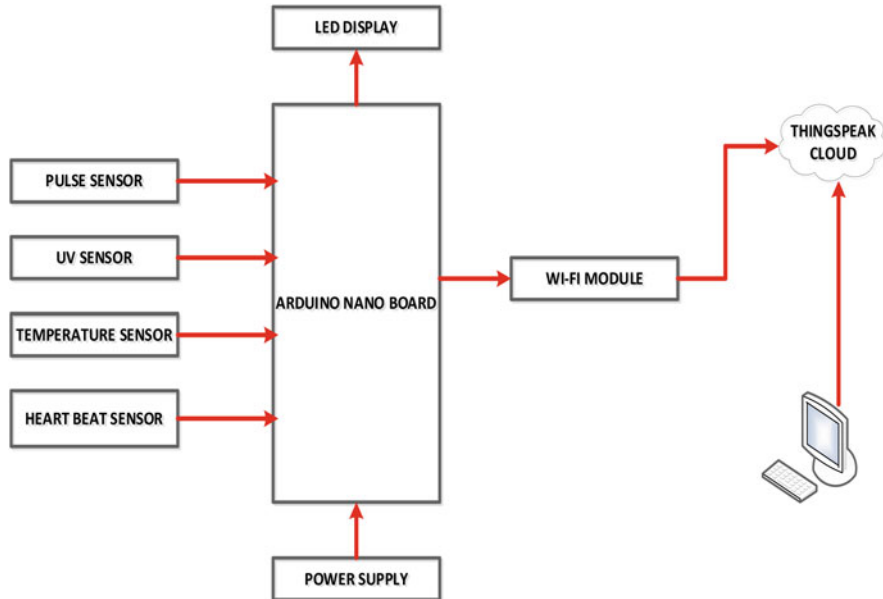
This study uses a phototransistor and an infrared LED to detect the finger's pulse, whereby a red LED flashes with each pulse. The finger's light side is the LED, while

**Table 1** Summary of related works

Author	Sensors	Methodology	Contribution	Limitation
Yeri and Shubhangi [41]	Temperature sensor, pulse sensor, and SpO2 sensor	Arduino, Wi-Fi, web, and mobile platform	The intervention time between doctor and patient is reduced in case of emergency Low cost	Proposed model doesn't include the blood pressure monitoring system
Hasan and Ismaeel [9]	ECG	Arduino Uno, ESP8266 Wi-Fi module, and Blynk IoT application		Absence of cloud database and limited parameters
Akshaya et al. [4]	Pulse/heartbeat sensor, temperature sensor, electrical sensor, blood pressure sensor, and patient position sensor	Raspberry Pi and Wi-Fi module	The proposed system was able to display data in real time	Data loss due to low signal gain
Rahman et al. [28]	ECG	Raspberry Pi	The proposed system was able to monitor the real-time status of the patient irrespective of the presence of the doctor	Limited parameter was considered
Warsi et al. [39]	Blood pressure, heartbeat rate, and ECG	Arduino and Wi-Fi module	The proposed system was able to upload the data to a cloud storage	Just three sensors were used for the analysis

Majumder et al. [15]	Blood pressure, heart rate, and temperature	Arduino and Bluetooth	Easily portable and cheaper	Need for additional sensory unit
Raiz [29]	Heartbeat	Microcontroller with Wi-Fi module	Low cost and high response rate	Limited parameter was considered
Sollu et al. [34]	Heartbeat and temperature	Raspberry Pi	Low cost	Distance of transmission is limited with obstruction
Bharadwaj et al. [5]	ECG and temperature	Arduino, Wi-Fi module, and ThingSpeak	Low cost	Limited parameter was considered
Li and Pan [11]	Temperature, ECG, and pulse rate	Bluetooth and GPRS	Portable and did not need extra communication network	Limited connectivity
Rajkumar et al. [26]	Temperature, heartbeat rate	Raspberry Pi	Low cost	Data are not easily accessible
Akhila et al. [3]	Temperature and heartbeat	Arduino and Wi-Fi module	Low cost	Limited parameters
Kumar and Rajasekaran [14]	Temperature sensor, heartbeat sensor, respiration sensor, and accelerometer sensor	Raspberry Pi	Effective transmission of patients' data	Limited connectivity
Tello et al. [35]	Temperature and ECG	Arduino and Bluetooth	Portability, low cost, connectivity easiness, and scalability	Delay in signals





**Fig. 1** Block diagram of the proposed system

on the other side of the finger is the phototransistor. The flux emitted while capturing the blood pressure pulse is obtained via the phototransistor. It is very critical to have a very sensitive phototransistor; therefore, we use a very high-resistance resistor. There are variations in the flow of blood in various parts of the veins, and luminosity variations are noticeable. The sensor can precisely calculate these variations, and the measured values are printed on the display unit. The technical specifications are as follows: resistance can be selected by experiment to get the best results; the stray shield light must be kept into the phototransistor.

### 3.3 Dallas Temperature Sensor DS18B20

The DS18B20 digital thermometer can measure up to 12-bit temperature measurement in Celsius. It is also incorporated with an alarm function that has a trigger point that is programmable by the user to hard-code its upper and lower trigger points. It transmits data to and from the central microprocessor via one data line, which also acts as a ground. This same data line is also used to power the thermometer with a technology known as “parasite power,” thereby reducing the circuitry of an external power source. Each DS18B20 has a unique 64-bit serial code, which allows

multiple DS18B20s to function on the same 1-Wire bus. This makes it easy to use a single microprocessor to control many DS18B20s scattered around a large area. The temperature sensor's technical specification is as follows: unique 1-Wire interface, measures temperature from  $-55$  to  $+125$  °C, power supply range of 3.0 V–5.5 V, and 9–12-bit selectable resolution.

### ***3.4 Ultraviolet (UV) Detection Sensor***

The ultraviolet sensor, commonly known as the UV sensor, is used to sense the magnitude of an incident UV radiation. Its electromagnetic radiation has a shorter wavelength than visible light. The UV sensor is based on the sensor GUVVA-S12D, which has a wide spectral range of 200–400 nm. The module generates an electrical pulse based on the intensity of the incident UV light.

### ***3.5 Liquid Crystal Display (LCD)***

This study utilizes a 16x2 LCD display, and it is basically used in DIYs and circuits. The 16x2 translates on display 16 characters per line in 2 of such lines. In this LCD, each character is displayed in a  $5 \times 7$ -pixel matrix. This is the visual output where all the commands made and decisions taken by the “brain,” the microcontroller unit (MCU), are displayed. It has 16 special pins that are mapped out for special functions. The data character is shown on the LCD.

### ***3.6 ESP8266-1 Wi-Fi Module***

The ESP8266-1 (ESP-01) is a Wi-Fi module that can allow a microcontroller (MCU) to have access to a Wi-Fi network. The module comes with a SOC (system on a chip), which means that it doesn't necessarily need a microcontroller to manipulate input and output pins. This gave the ESP-01 properties to act like a small computer. The ESP-01 has nine GPIOs (general-purpose input/output). With the ESP-01 module acting as a module as it is connected to the MCU in station (STA) mode, we can have Internet access once we are connected to the Wi-Fi network. The ESP8266 Wi-Fi module is a module that can connect to the Internet. The technical specifications are as follows: 802.11b/g/n, Wi-Fi Direct, 1 MB flash memory, SDIO 1.1/2.0, SPI, and UART.

**Table 2** Technical specifications for the Arduino Nano

Description	Specification
Microcontroller	ATmega328P 8-bit AVR family microcontroller
Operating voltage	5 V
Recommended input voltage for vin pin	7–12 V
Analog input pins	6 (A0–A5)
Digital I/O pins	14 (out of which 6 provide PWM output)
DC current on I/O pins	40 mA
DC current on 3.3 V pin	50 mA
Flash memory	32 KB (2 KB is used for bootloader)
SRAM	2 KB
EEPROM	1 KB
Frequency (clock speed)	16 MHz
Communication	IIC, SPI, USART

### 3.7 *Microcontroller Unit*

Arduino microcontroller ATmega328P 8-bit will be used to control the circuit and get the desired output. The code for the microcontroller was written in C using the Arduino IDE to read ECG, temperature, heartbeat rate, and pulse rate. The code was first tested and reviewed for bugs via the IDE and transferred to the microcontroller via the IDE. Data is processed and transmitted serially to the ESP8266 Wi-Fi module. The integration test and the logical error test of the code were performed during the hardware device simulation. The technical specification according to the datasheet is described in the table below (Table 2).

### 3.8 *Proposed System Circuit Design*

The LCD connection was made using 4-bit data connection. The register select (RS) connection is connected to digital pin 13. The wiper of the potentiometer is connected to Vo. The Enable (E) pin is connected to digital pin 12 on the Uno board. The 4-bit data pins (D4–D7) are connected to digital pin 9 through 6. The read/write (RW) is grounded. The buck converter module was used to shift the voltage level from 5 V to 3.3 V for the ESP-01 module. The ESP-01 module won't work on 5 V and usually gets hot and would burn out on long usage when powered by 5 V. All ground pins are connected to the ground.

The sensors are connected to the analog IOs of the microcontroller board. At the same time, the UV sensor is connected to the SPI pins, which are the analog pins 4 and 5. The circuit layout comprised of four sensors and was developed using the circuit design program called Fritzing; the components were connected to the Arduino via jumper cables. Arduino is interfacing with various modules

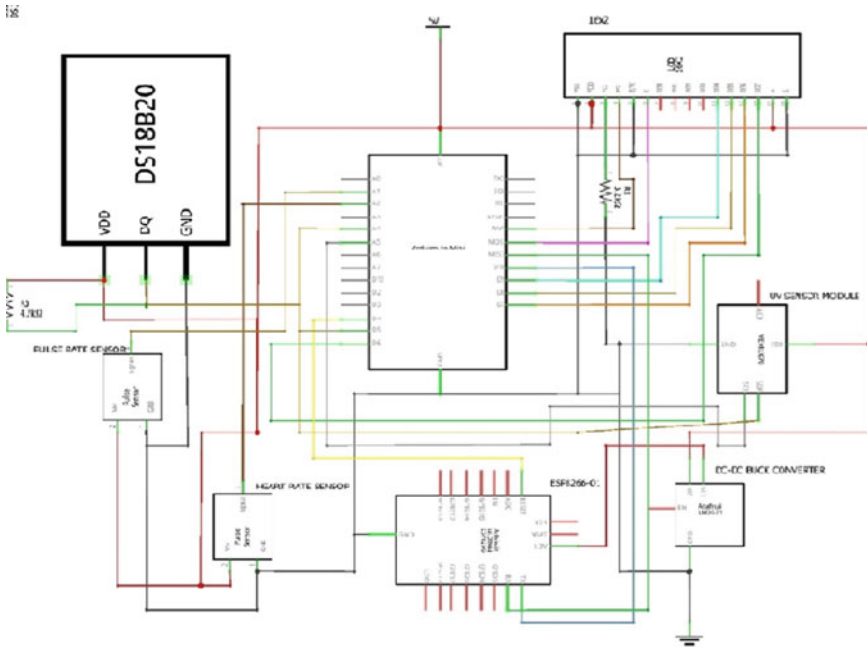


Fig. 2 Schematic diagram of the proposed system

such as LCD, Wi-Fi, temperature sensor, heartbeat sensor, ECG sensor, and pulse sensor. Communication between the sensors and the Arduino was transmitted to the ThingSpeak cloud through the ESP8266-1 Wi-Fi module. The Wi-Fi module will keep giving detailed information of the person’s heartbeat at the exact time. Figure 2 shows how the sensors are interfacing with the Arduino Nano; it also shows the ESP8266-1 Wi-Fi access module’s role in communicating with the Arduino.

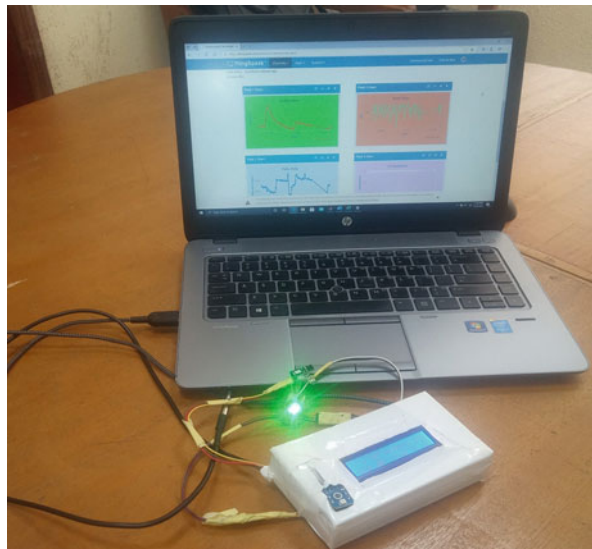
### 3.9 Web Application

ThingSpeak is a very popular GUI-based analytical software tool for IoT applications. It can help the user analyze and have visuals of live streams of data as received in real time. Once connected, the monitoring of data happens instantly. Most of the times the ThingSpeak application can be interfaced with different microprocessor technologies, such as the Raspberry Pi, Arduino, and any other hardware devices. If there is any application that requires the logging of data from a sensor device, ThingSpeak will make that data come alive [5]. Figure 3 shows the layout of the ThingSpeak web application for the proposed system.



Fig. 3 ThingSpeak web application for the proposed system

Fig. 4 Proposed system prototype



In order to effectively send data to ThingSpeak using an Arduino, the ThingSpeak needs a user account and a channel. The basic steps to follow while using [thingspeak.com](https://thingspeak.com) are:

- Step 1: Collect the data in the new channel.
- Step 2: Analyze your data.
- Step 3: Act on your data.

The proposed system prototype is shown in Fig. 4.

Figure 4 shows a working prototype of the proposed health monitoring system. The universal serial bus from the Arduino is connected to a power supply. The default serial communication pins of the Arduino are 0 and 1. Once powered up, the PC's mobile hotspot's name and password have been configured to match the ESP8266-1 Wi-Fi access module configuration. The patients place their fingers on

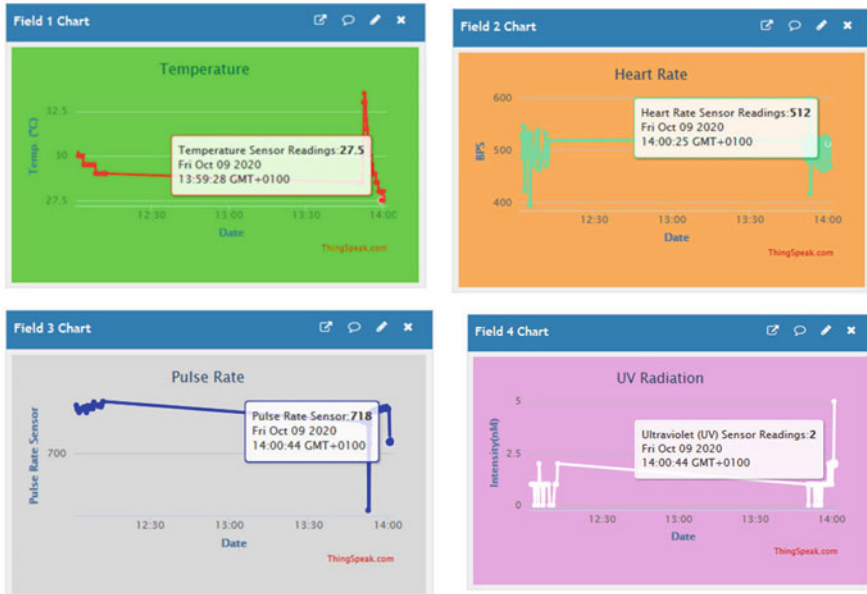


Fig. 5 Health vitals chart of user 1

each of the different sensors, and the readings are displayed on the LCD screen. The ESP8266-1 Wi-Fi access module transmits these readings to the ThingSpeak cloud. The communication is made through virtual serial ports created in a computer. On the other hand, the doctor logs into the ThingSpeak cloud platform and views the different readings of each sensor of the patients.

### 4 Results and Analysis

The outputs from the sensors were connected to Arduino and successfully sent via Wi-Di module. The output in Figs. 5, 6 and 7 depicted the given live temperature, heartbeat, pulse rate, and UV readings, which can be viewed through the cloud (IoT, thingspeak.com). The output reading was displayed at a rate of 7 seconds as depicted in Table 3.

Table 3 shows the average number of seconds taken for the readings gotten from the sensors to be uploaded to the ThingSpeak cloud.

After each patient takes their readings, the doctor logs into the ThingSpeak web application through [www.thingspeak.com](http://www.thingspeak.com) to view the health parameters of each patient. The different charts in Figs. 5, 6 and 7 show the different readings of each sensor for different patients taken in real time. With the readings for each sensor on the y-axis and date and time on the x-axis, the graphs were plotted. Each dot

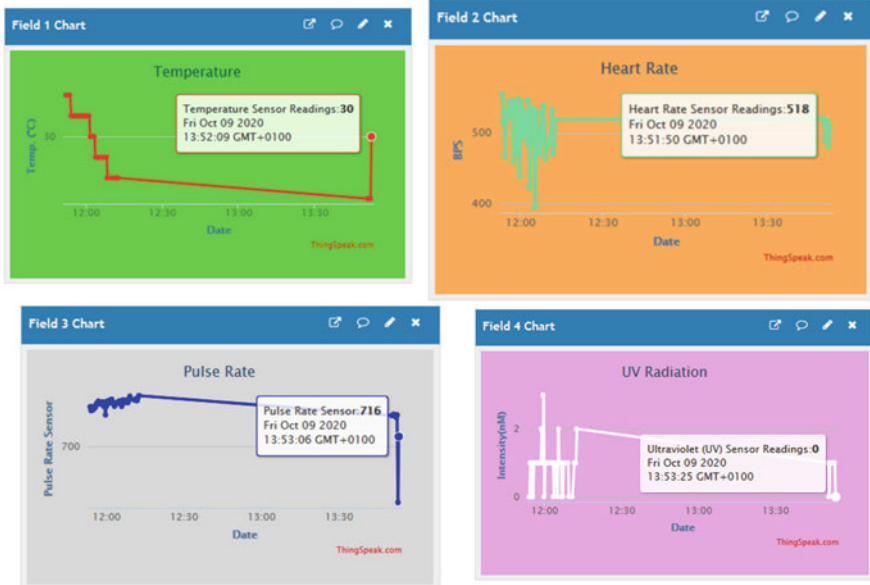


Fig. 6 Health vitals chart of user 2

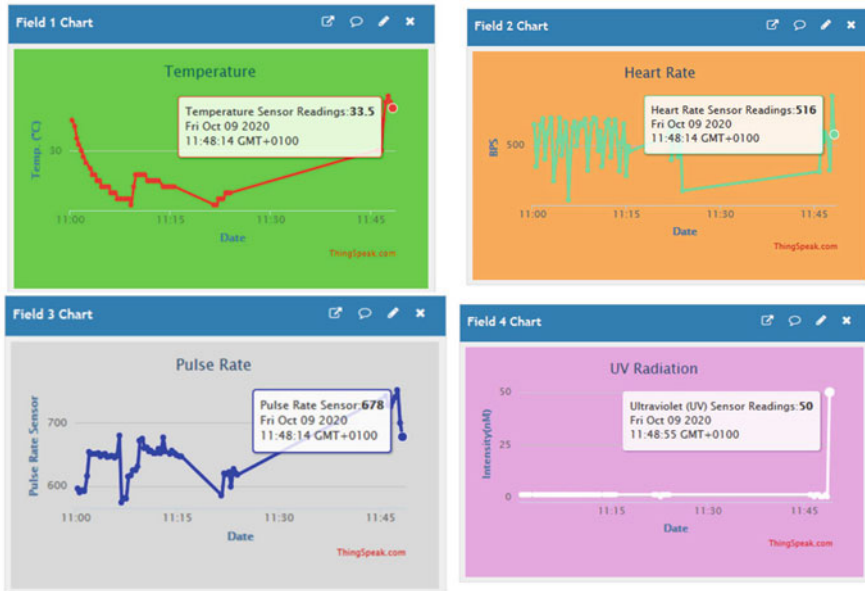


Fig. 7 Health vitals chart of user 3

**Table 3** Responses of the sensors

Sensors	Trial 1 (Seconds)	Trial 2 (Seconds)	Trial 3 (Seconds)	Average time (Seconds)
Temperature	7	7	7	7
Heartbeat	7	7	7	7
Pulse rate	7	7	7	7
UV	7	7	7	7

	created_at	entry_id	Temperature	Heart Rate	Pulse Rate	UV Sensor
2	2020-09-10 12:05:16 UTC	381	28	493	782	0
3	2020-09-10 12:05:35 UTC	382	28	519	785	0
4	2020-09-10 12:05:55 UTC	383	28	497	779	0
5	2020-09-10 12:06:14 UTC	384	28	480	784	0
6	2020-09-10 12:06:33 UTC	385	28	514	779	0
7	2020-09-10 12:06:52 UTC	386	28	518	782	0
8	2020-09-10 12:07:11 UTC	387	28	508	781	0
9	2020-09-10 12:07:31 UTC	388	28	517	779	1
10	2020-09-10 12:07:50 UTC	389	28	513	781	0
11	2020-09-10 12:08:09 UTC	390	28	519	781	0
12	2020-09-10 12:08:28 UTC	391	28	487	782	0
13	2020-09-10 12:08:47 UTC	392	28	522	781	0
14	2020-09-10 12:09:07 UTC	393	28	518	782	0
15	2020-09-10 12:09:26 UTC	394	28	504	784	0
16	2020-09-10 12:09:45 UTC	395	28	486	780	0
17	2020-09-10 12:10:04 UTC	396	29	514	777	0
18	2020-09-10 12:10:23 UTC	397	34	522	776	0
19	2020-09-10 12:10:42 UTC	398	32.5	442	772	0
20	2020-09-10 12:11:01 UTC	399	31.5	561	785	0
21	2020-09-10 12:11:20 UTC	400	31.5	755	776	0
22	2020-09-10 12:11:39 UTC	401	31	502	771	0
23	2020-09-10 12:11:58 UTC	402	30.5	516	772	0

**Fig. 8** Patient data stored on the ThingSpeak cloud for export

on the chart shows a reading taken by the sensor together with the date and time. The readings gotten from the sensors are automatically uploaded to the ThingSpeak cloud, and these helps doctors to easily access a patient data from months or years ago. These data stored on the cloud can easily be downloaded and exported to another platform for offline availability of patient’s data. The export data is in Microsoft Excel format, as depicted in Fig. 8.

### 4.1 Comparison with Existing Work

Table 4 shows the comparison of the proposed prototype with the previous work on health monitoring system. Our prototype considered four parameters (temperature, UV, pulse rate, and heartbeat), whereas the device designed by [41] considered three parameters. The device designed by [9] focused only on ECG, and there is absence of cloud platform. The work carried out by [28] also considered limited parameters, and there is no cloud storage. The comparison table shows the various



**Table 4** Comparison with existing work

Authors	No of parameter measured	Cloud platform	Statistical analysis
Yeri and Shubhangi [41]	3	Yes	Nil
Hasan and Ismaeel [9]	1	No	Nil
Rahman et al. [28]	1	No	Nil
Warsi et al. [39]	3	Yes	Nil
Our work	4	Yes	Response time

physiological parameters measured. Some drawbacks of the existing methods are the use of limited parameters and also lack of evaluation. One major drawback of our proposed health monitoring system is that it is not portable.

## 5 Conclusion

The use of remote patient health monitoring system innovation based on IoT that enabled patient observations outside clinical settings cannot be overemphasized. Generally, IoT provides a new approach to health and patient care with remote monitoring. This study is focused on implementing an enhanced health monitoring system that can measure various vital signs (pulse rate, temperature, heartbeat rate, and UV) of patients/users that can be transmitted in real time over the Internet. This study effectively developed a cheap but efficient system of monitoring the health vitals of people without them needing to go to the hospital for regular checkups. In order to achieve this, the system is built on Arduino ATmega328P 8-bit. The 16x2 LCD displays the readings from the integrated sensory units that measure the vital signs of patients.

The proposed system is IoT-enabled so that patient reading is seamlessly relayed to a cloud environment ([thingspeak.com](https://thingspeak.com)) via an ESP8266-1 Wi-Fi module, which allows a microcontroller to have access to a Wi-Fi network. The doctors are able to log in to the IoT platform to monitor the vital signs of patients and view the readings from each of the sensors. Experimental results show that the health monitoring system effectively and efficiently monitors patients' vital signs with a response time (i.e., the time it takes to display on the LCD) of 7 s consecutively for each of the three trials for all of the sensory units (temperature sensor, pulse rate sensor, heartbeat sensor, and UV sensor). The acquired readings are further automatically loaded and uploaded to the ThingSpeak cloud.

Hence, the proposed system is a low-cost system that eliminates the need of constantly going to the hospital for checkups and where doctors are able to monitor their patient health in real time by focusing on their temperature, pulse rate, heartbeat, and UV. From the evaluation and the results of analysis, the system is very efficient. However, there is room for improvement; in the future, the system can be extended by adding few parameters (ECG, body mass index, and glucose levels

can be added to the proposed systems for a concise vital signs of the patients). The working prototype can also be developed into a wearable device to allow for efficient portability. A mobile application can also be created so that doctors receive SMS alerts in the event of emergency and critical cases.

## References

1. D. Adeloje, T. Adigun, S. Misra, N. Omoregbe, Assessing the coverage of E-health Services in sub-Saharan Africa. *Methods Inf. Med.* **56**(3), 189–199 (2017)
2. P. Ajayi, N. Omoregbe, S. Misra, D. Adeloje, Evaluation of a cloud based health information system, in *Innovation and Interdisciplinary Solutions for Underserved Areas. CNRIA 2017, InterSol 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, ed. by C. M. F. Kebe, A. Gueye, A. Ndiaye, vol. 204, (Springer, 2018), pp. 165–176. LNICST
3. V. Akhila, Y. Vasavi, K. Nissie, P.V. Rao, An IoT based patient health monitoring system using Arduino Uno. *Int. J. Res. Inf. Technol.* **1**(1), 1–9 (2017)
4. S.B. Akshaya, G. Anil, R. Paulson, R.J. Abraham, P. Vandana, IoT based health monitoring system. *Int. J. Res.Eng. Sci. Manag.* **2**(6), 2581–5792 (2019)
5. K. Bharadwaj, R. Dhawan, M.K. Ray, P. Mahalakshmi, Wi-fi-based low-cost monitoring of ECG and temperature parameters using Arduino and ThingSpeak, in *Advances in Systems, Control and Automation*, (Springer, Singapore, 2018), pp. 637–646
6. A. Deepa, P.N. Kumar, Patient health monitoring based on ZigBee module, in *2013 International Conference on Optical Imaging Sensor and Security (ICOSS)*, (IEEE, 2013, July), pp. 1–4
7. D. Gil, M. Johnsson, H. Mora, J. Szymański, Review of the complexity of managing big data of the internet of things. *Complexity* **2019**, 1–13 (2019)
8. H. Habibzadeh, C. Kaptan, T. Soyata, B. Kantarci, A. Boukerche, Smart City system design: A comprehensive study of the application and data planes. *ACM Comput. Surv. (CSUR)* **52**(2), 1–38 (2019)
9. D. Hasan, A. Ismaeel, Designing ECG monitoring healthcare system based on internet of things Blynk application. *J. Appl. Sci. Technol. Trends* **1**(3), 106–111 (2020)
10. I.J. Hoque, M. Navid, R.B. Reza, M.I. Mahub, IoT Based Patient Monitoring System (Doctoral dissertation, BRAC University) (2018)
11. H. Li, T. Pan, Development of physiological parameters monitoring system using the internet of things. *Int. J. Online Biomed. Eng. (iJOE)* **13**(09), 87–100 (2017)
12. A. Khanna, S. Kaur, Evolution of internet of things (IoT) and its significant impact in the field of precision agriculture. *Comput. Electron. Agric.* **157**, 218–231 (2019)
13. S. Kumar, P. Pandey, A smart healthcare monitoring system using smartphone interface, in *2018 4th International Conference on Devices, Circuits and Systems (ICDCS)*, (IEEE, 2018, March), pp. 228–231
14. R. Kumar, M.P. Rajasekaran, An IoT based patient monitoring system using raspberry Pi, in *2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16)*, (IEEE, 2016, January), pp. 1–4
15. S. Majumder, M.A. Rahman, M.S. Islam, D. Ghosh, Design and implementation of a wireless health monitoring system for remotely located patients, in *2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEICT)*, (IEEE, 2018, September), pp. 86–91
16. G. Marques, R. Pitarma, mHealth: Indoor environmental quality measuring system for enhanced health and well-being based on internet of things. *J. Sens. Actuator Netw.* **8**(3), 43 (2019)

17. J. Nagy, J. Oláh, E. Erdei, D. Máté, J. Popp, The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain—The case of Hungary. *Sustainability* **10**(10), 3491 (2018)
18. A.H. Najar, Internet of things (IoT): Security issues and challenges. *Int. J. Manag. IT Eng.* **9**(3), 248–260 (2019)
19. M.R.F. Nurdin, S. Hadiyoso, A. Rizal, A low-cost internet of things (IoT) system for multi-patient ECG's monitoring, in *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, (IEEE, 2016, September), pp. 7–11
20. N.A. Omoregbe, I.O. Ndaman, S. Misra, O.O. Abayomi-Alli, R. Damaševičius, Text messaging-based medical diagnosis using natural language processing and fuzzy logic. *J. Healthc. Eng.* **2020**, 8839524 (2020)
21. I. Osebor, S. Misra, N. Omoregbe, A. Adewumi, L. Fernandez-Sanz, Experimental simulation-based performance evaluation of an sms-based emergency geolocation notification system. *J. Healthc. Eng.* **2017**, Article ID 7695045, 12 pages (2017)
22. M. Park, H. Oh, K. Lee, Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors* **19**(9), 2148 (2019)
23. E.G. Petrakis, S. Sotiriadis, T. Soultanopoulos, P.T. Renta, R. Buyya, N. Bessis, Internet of things as a service (iTaaS): Challenges and solutions for Management of Sensor Data on the cloud and the fog. *Internet of Things* **3**, 156–174 (2018)
24. R.R. Prasad, S. Paudel, Impacts of air pollution on epidemiology and cardiovascular systems, in *Air Pollution and Environmental Health*, (Springer, Singapore, 2020), pp. 179–207
25. P.P. Singh, Zigbee and GSM based patient health monitoring system. In: *2014 International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, (2014), pp. 1–5
26. S. Rajkumar, M. Srikanth, N. Ramasubramanian, Health monitoring system using raspberry PI, in *2017 International Conference on Big Data, IoT and Data Science (BIGD)*, (IEEE, 2017, December), pp. 116–119
27. B.P. Rao, P. Saluia, N. Sharma, A. Mittal, S.V. Sharma, Cloud computing for internet of things & sensing based applications, in *2012 Sixth International Conference on Sensing Technology (ICST)*, (IEEE, 2012, December), pp. 374–380
28. A. Rahman, T. Rahman, N.H. Ghani, S. Hossain, J. Uddin, IoT based patient monitoring system using ECG sensor, in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, (IEEE, 2019, January), pp. 378–382
29. Riaz, M., 2018. Design and Fabrication of Arduino Based Heart Rate Monitoring System Using Reflectance Photoplethysmography
30. G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology, in *Multimedia Tools and Applications*, (2019), pp. 1–23
31. V.M. Santos, S. Misra, M.S. Soares, Architecture conceptualization for health information systems using ISO/IEC/IEEE 42020. *Lect. Notes Comput. Sci* **12254**, 398–411 (2020, July). LNCS
32. M. Singh, N. Jain, Performance and evaluation of smartphone based wireless blood pressure monitoring system using Bluetooth. *IEEE Sensors J.* **16**(23), 8322–8328 (2016)
33. P. Sivasankari, M. Anbarasan, M. Moses, Arduino based human health care monitoring and control system. *IOSR J. Electr. Electron. Eng.* **11**(3), 9–18 (2016)
34. T.S. Sollar, M. Bachtiar, B. Bontong, Monitoring system heartbeat and body temperature using raspberry pi, in *E3S Web of Conferences*, vol. 73, (EDP Sciences, 2018), p. 12003
35. P.J.P. Tello, O. Manjarres, M. Quijano, A.U. Blanco, Remote monitoring system of ECG and temperature signals using Bluetooth, in *2012 International Symposium on Information Technologies in Medicine and Education*, vol. 2, (IEEE, 2012, August), pp. 860–863
36. M.S. Uddin, J.B. Alam, S. Banu, Real time patient monitoring system based on internet of things, in *2017 4th International Conference on Advances in Electrical Engineering (ICAEE)*, (IEEE, 2017, September), pp. 516–521

37. P. Verma, S.K. Sood, Fog assisted-IoT enabled patient health monitoring in smart homes. *IEEE Internet Things J.* **5**(3), 1789–1796 (2018)
38. V. Vippalapalli, S. Ananthula, Internet of things (IoT) based smart health care system, in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, (IEEE, 2016, October), pp. 1229–1233
39. G.G. Warsi, K. Hans, S.K. Khatri, IOT based remote patient health monitoring system, in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, (IEEE, 2019, February), pp. 295–299
40. A. Yassine, S. Singh, M.S. Hossain, G. Muhammad, IoT big data analytics for smart homes with fog and cloud computing. *Futur. Gener. Comput. Syst.* **91**, 563–573 (2019)
41. V. Yeri, D.C. Shubhangi, IoT based real time health monitoring, in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, (IEEE, 2020, July), pp. 980–984
42. S. Zafar, G. Miraj, R. Baloch, D. Murtaza, K. Arshad, An IoT based real-time environmental monitoring system using Arduino and cloud service. *Eng. Technol. Appl. Sci. Res.* **8**(4), 3238–3242 (2018)
43. N.I. Zainal, M.Z.M. Rodzi, S. Khan, M.H. Habaebi, T.S. Gunawan, Design and development of wireless PPG data acquisition for health monitoring application using Bluetooth module, in *2016 IEEE Student Conference on Research and Development (SCOReD)*, (IEEE, 2016, December), pp. 1–6
44. M. Zubair, D. Unal, A. Al-Ali, A. Shikfa, Exploiting bluetooth vulnerabilities in e-health IoT devices, in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, (2019, July), pp. 1–7

# A Secured Smart Healthcare Monitoring Systems Using Blockchain Technology



Joseph Bamidele Awotunde , Chinmay Chakraborty ,  
and Sakinat Oluwabukonla Folorunso 

## 1 Introduction

The introduction of new technologies has contributed to the innovations in smart healthcare systems especially the Internet of Things (IoT), interconnected devices, and medical sensors to promote knowledge gathering, storage, communication, and sharing. The dramatic change in traditional healthcare systems into a smarter healthcare system using various wireless technologies as a catalyst like wearable sensors, wireless sensor networks, RFID, Bluetooth, Li-Fi, and Wi-Fi among others has greatly helped and changed the medical sectors [1, 2]. In recent years, the use of IoT has penetrated all fields such as agriculture, education, transportation, and most especially the healthcare sectors, thus paving the way toward technological transformations [3, 4]. There has been tremendous growth in the healthcare system using IoT-based devices to achieve a great level of automation. To obtain universal and holistic healthcare services, we are countersigning the beginning of smart healthcare systems with possible and the possibility for improvement where all stakeholders are interconnected using IoT-based devices.

This new emergence of these technologies is a result of their high availability, simplicity to personalize, and easy accessibility, thus enabling the providers to

---

J. B. Awotunde (✉)

Department of Computer Science, University of Ilorin, Ilorin, Nigeria  
e-mail: [awotunde.jb@unilorin.edu.ng](mailto:awotunde.jb@unilorin.edu.ng)

C. Chakraborty

Department of Electronics and Communication Engineering, Birla Institute of Technology,  
Jharkhand, India  
e-mail: [cchakraborty@bitmesra.ac.in](mailto:cchakraborty@bitmesra.ac.in)

S. O. Folorunso

Department of Mathematical Sciences, Olabisi Onabanjo University, Ago-Iwoye, Nigeria  
e-mail: [sakinat.folorunso@oouagoye.edu.ng](mailto:sakinat.folorunso@oouagoye.edu.ng)

deliver personalized content cost-effectively on a large scale easily. Also, big data analytics and IoT are progressively gaining more attraction for the next generation of mHealth and eHealth facilities. While the new technologies the new fields evolving rapidly, they also have their shortcomings, particularly when the goal is healthcare systems with a complicated problem, difficult in energy-efficient, safe, flexible, suitable, and consistent solutions. These challenges becomes serious especially when it comes to the issue of security and privacy of IoT-based system generally. It has been projected that IoT will rise to a market scope of \$300B by 2022 in healthcare covering the medical devices, systems, applications, and services sectors [5]. IoT allows a broad range of intelligent applications and resources to solve the problems facing individuals or the healthcare sector [6]. For instance, P to D (Patient-to-Doctor), P to M (Patient to Machine), S to M (Sensor to Mobile), M to H (Mobile to Human), D to M (Device to Machine), O to O (Object to Object), D to M (Doctor to Machine), and T to R (Tag to Reader) have dynamic IoT link capabilities. This brings people, computers, smart devices, and complex systems together intelligently to ensure a productive healthcare system [7, 8].

In recent years, blockchain technology has demonstrated its tremendous adaptability as a range of business sectors have found ways to incorporate its capabilities into their operations. Although much of the emphasis has been on the financial services sector so far, many projects are starting to shift to other service-related fields like healthcare. Blockchain is a rapidly evolving technological technology that has piqued the attention of people all over the world. This technology makes electronic medical data transmission faster and safer than the traditional method. It's common knowledge that blockchain can help protect and simplify healthcare data. Because of the enhanced protection and privacy of clients on medical apps, the emerging technology addresses the requirements of creating a stable application for a smart healthcare system.

A decentralized database that continuously kept up-to-date patient's information provides the healthcare sector with many benefits. When various parties require access to the same information, these benefits become particularly interesting. For instance, regarding the care of the elderly or chronic diseases, medical treatment processes are vital areas in a healthcare system where blockchain technology can be helpful. Especially where there are many parties involved like physicians, hospitals, druggist, therapists, etc., and huge media disruptions involved during the treatment of a patient. A variety of involved parties (like therapists, general practitioners, hospitals, medical specialists, etc.) and the rate of media disruptions like MHRs, mismatched IT interfaces among other intricates through the patient's therapy can be laborious and resource-intensive authentication and information processes for all medical stakeholders (Fig. 1).

Blockchain technology has proven to be effective with the privacy and security of companies' data and information. The blockchain can be used to record from beginning to the present state in unchangeable log events of a commodity or subject encounters. The testing of the newness of food, the ownership of various proprieties, and the authenticity of materials are some instances of usage of blockchain. The enforcement of smart contacts in blockchain is now possible in IoT-based systems

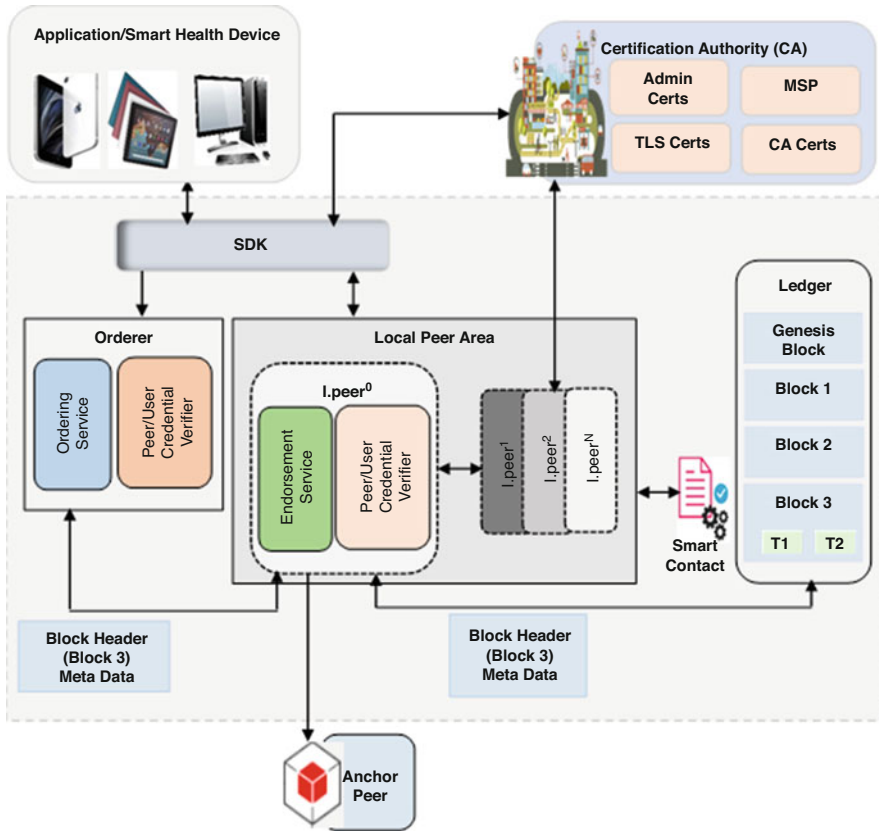


Fig. 1 The blockchain framework for transaction in a smart healthcare system

with code that can be implemented by triggers automatically based on predefined conditions. The smart contracts can cause warnings for any suspicious behaviors to automated analysis of health data captured based on custom threshold values using WBAN devices for every patient. The order of transmissions from WBAN node to support smart contracts in blockchain should hold a permanent record to monitor information regarding measurements taken and given treatment commands. In the safety and confidentiality of healthcare information records, cost saving, and healthcare monitoring, blockchain has greatly contributed to healthcare sectors.

Although there are numerous security protocols, like encryption and other security implementations, MAC techniques, public-key cryptography, k-anonymity, and many more [9–11] secure data from threats/attacks. When relating them to IoT-based health systems, they also have distinctive boundaries based on processor enactment, cost of energy and device, etc. While many current works provide data privacy protection over contact to patients, when a cloud service has been agreed upon, they do not protect the data, particularly when a cloud service is threatened by

an employee or service vendor. The IoT model also needs appropriate clarifications to safeguard patient information from Internet threats/strikes from sensing devices to healthcare providers. This study consequently discusses the issues of privacy and security in IoT healthcare systems and provides an overview of IoT, including its architectural design. The chapter also suggested a framework to secure healthcare information in the IoT environment.

Therefore, this chapter proposed a framework for a secured smart healthcare system using blockchain. Privacy and authenticity are important when working with smart healthcare systems. Blockchain distributed ledger was used in the framework for legitimacy and endorsement while preserving anonymity through authorized management of consortia and anonymized accounts. Only the approved individuals can access block verification and inspection in the blockchain when compared with the traditional methods of using civic blockchain like Bitcoin. They will also own a nameless account for each registered user, which can only be tracked at their discretion. This encourages patient accountability and helps them to better monitor their data on healthcare.

The other part of the chapter is as follows: Sect. 2 discusses IoT-based challenges in the smart healthcare system. Section 3 presents the applications of blockchain in a smart healthcare system. Section 4 presents the challenges of applying blockchain in a smart healthcare system. Section 5 presents the architecture for a secured smart healthcare monitoring system using blockchain. Lastly, Sect. 6 concludes the chapter and discusses forthcoming works for the realization of efficient uses of the framework in healthcare systems.

## **2 Internet of Thing-Based Challenges in Smart Healthcare System**

With new emerged technologies like medical sensors to remotely monitor patients, wearable technology for the IoT-based system has unfolded new opportunities in the medical field. Wireless Body Area Network (WBAN) is a subset of IoT healthcare patterns. To monitor the vital physiological part of the human body, various embedded and implanted devices have recently been used like measuring heart rates and glucose levels in real time. There are other devices and sensors that can provide automated care and treatment acting like an actuator's measurement. The captured data report to a cell phone serves as a storage device and relays the data gathered to healthcare workers for a prompt response to users' demands. This remote monitoring removes the call for doctors and encourages patients to move more easily in their everyday lives [12].

Remote patient monitoring is increasingly rising in popularity. In 2016, 7.1 million outpatients globally outsourced their health management plan to remote monitoring, and it is expected to reach 50.2million by 2021 [13]. Furthermore, in the USA, as of January 1, 2018, the Centers for Medicare & Medicaid Programs



announced new payment incentives that enable the use of “active feedback loop” devices that deliver real-time observation [14]. If the area of remote patient monitoring grows, there are concerns regarding the accurate and safe transfer of medical data. Measurements obtained from various sensors must be aggregated, formatted, and processed together to provide integrated health monitoring. The hackers’ main target is the health data; thus, there is a need to safeguard the transmission of protected health information (PHI) through government regulation. Therefore, it is important to protect patient privacy, and electronic health records (EHRs) must be conveniently manageable and portable.

Recent technological developments have greatly changed the understanding of an individual’s conventional way of conducting day-to-day operations. In the real world, including the healthcare background, the Internet of Things has to be a rising trend in different segments. This rapid IoT revolution, however, has also generated some uncertainties and concerns about the protection of data that is stored in different connected items. If the number of items such as sensors and computers increases, it becomes more difficult to maintain robust protection and the privacy of sensitive data.

These protection and privacy problems are the products of worsening the efficacy of healthcare systems dependent on the IoT and adversely affecting the confidential health information of individuals. Since healthcare data is important and sensitive, the IoT healthcare paradigm’s protection of security and privacy makes matters even more problematic. While evolving IoT paradigms in the medical system contribute significantly to the advancement of current healthcare systems, end users need to address many privacy and security concerns. When they grant authorization for potentially insecure or leaky third-party applications, end users may be susceptible to malicious threats. Since the data is transferred to the cloud, it moves through unsafe communication networks, many of which have security issues. Besides, when the data projects into the cloud storage facility of the owner, there are alternate data breach issues.

To enhance the comfort of patients concerning the protection and secrecy dangers hackers pose to the lives of patients and other effects, the protection of IoT-based systems is very necessary. Through reviewing the components of the technology platform in depth, the privacy and security problems of IoT-based systems are the focus of this chapter. Remote patient management processes and warning systems are assisted by healthcare providers and applications. Data is the most valuable asset of these applications as knowledge obtained through these processes is known to be vulnerable [15, 16]. The confidentiality and prompts for the availability of medical data are very important. Sensitive data should be protected, as should protect against unlawful entry, other challenges, and risks. Conversely, due to the amount of data provided by the wearable sensors and the constant interaction between the devices in the system [16], these are difficult areas in the IoT ecosystem. Healthcare practitioners and software developers have worked together in recent years to create stable IoT healthcare applications to solve these problems [15].

Also, the inherent difficulties impede the services offered by IoT technology. The problems often prevent patients from implementing smart healthcare systems,

taking into account the problems posed by privacy and security issues [17]. In a device concerned with confidential data, trust is also a crucial factor. Therefore, it would increase the performance of the programs and loyalty between clients by creating a layout that addresses the entire threat landscape. As a result, IoT healthcare will encourage more individuals to benefit from it [15]. Security is also a primary prerequisite for healthcare applications. For ethical and legal purposes, the effectiveness of healthcare applications depends primarily on patient protection and privacy [18, 19].

However, in terms of information safety and confidentiality, the sum of related gadgets and the huge sum of impressionable datasets gathered by those gadgets have brought novel challenges. Cyberattacks have also changed along with the rapid development of IoT and had created a recent avenue of invasion and risk to the whole medical industry. Many studies explored IoT's numerous privacy and protection issues and device weaknesses in cloud and fog computing settings relevant to IoT-based medical management gadgets [20, 21] and [20] analyzed the IoMT protection and confidentiality taxonomy in detail.

The safety and confidentiality of records relating to patients are twofold essential notions. When we refer to record safety, this signifies that records are securely stowed and transmitted to ensure their absoluteness, genuineness, and legitimacy. Record confidentiality signifies that records can solitarily be obtained by individuals who are authorized to sight and utilize it [22, 23]. More rational security measures may be established with different objectives and specifications in mind. The extensive utilization of IoT gadgets offers an improved assurance of an individual's health [24], but it also places a great deal of demand on record safety and concealment.

The most critical problem is data privacy in the IoT. The patient's body carries the sensors used in the IoT. These sensors are sensed by all significant information about the patient. So, sensitive information of the patient should not be leaked in the external world. The sensor nodes in IoT-based healthcare applications collect the patient's sensitive data and forward it to a coordinator node. If the sensitive information is overheard by an attacker and the data is used for any illicit reason, then the patient may be seriously harmed. It's not enough to only protect secrecy [25, 26].

Data should also be safe from outside modifications. In this case, if a patient's sensitive and essential data has been corrupted, this changed data will be transmitted to the coordinator. For life-critical patients, this lack of honesty results in serious harm. Data loss can also occur in poor communication environments. In terms of performance and security, the implementation of emerging technology poses many challenges; thus, applications for the IoT must be secured. It can have deadly consequences to reveal any part of an IoT healthcare system for hacking, cyberterrorism, disgruntled individual, blackmailing, or any other harmful act. As researches into the security of IoT are emerging, it is pertinent to know the extent of risk to be borne by ethicists and medical, legal, security, and finance professionals.

### 3 Application of Blockchain in Smart Healthcare System

Smart healthcare and biomedical novelty affect scientific advancement that is seaming out worldwide to be uplifted in all directions. It is exclusively important to improve the structure, trust, protocol, and effectiveness of healthcare facilities and to provide patients with skilled diagnosis, treatment, and care. In this day and age, until a big hardship occurs, people are more hesitant to access personal health insurance. It was discovered that patients do not go to clinics for a medical checkup until things get out of hand; such a thing can also be viewed as an over-engagement category with the busy life and tuned lifestyle system of the consumer. Hence, if a system is designed such that a person's health status can be measured or detect anybody's irregularities and can report to the person's assigned caregiver or personal healthcare supervisor, then the entire scenario can be much more convenient, and the patient can also be contacted effortlessly at the right time and within a sheltered span.

Information security, privacy, completeness, and access must be taken with all seriousness in healthcare services. This amplifies importance of healthcare cost control is another area that the massive healthcare industry can look into. The healthcare services have enjoyed utmost security and privacy with the promise of blockchain combined with IoT-based application layers built atop by guaranteeing that applicable users can access a continuous record of information. Blockchain has increased stakeholders' accessibility to medical information and reduced cost by breaking third-party brokers' involvement in any financial transactions, thus reducing healthcare costs and potentially giving better results [27]. The researchers are looking to areas of applying blockchain technology to solve real-world problems like healthcare diagnosis and monitoring systems, centralize research data, reduce healthcare overhead cost, and organize patient data from huge input big data. The described, touch on near-term promise and challenges are concrete examples of blockchain technology application in healthcare systems [27].

To remove the need for a trusted third party to validate and notarize transactions, blockchain technology has been used for money exchange transactions, as well as to protect data protection and privacy during the transactions. In other sectors like the healthcare system, education, transportation, electricity, and tourism, new blockchain structures have been developed to meet the need for these fields. Healthcare systems as part of the IoT-based model are projected to produce trillions of dollars over the next decade [28]. More significantly, smart healthcare has shown a substantial decrease in mortality rates and healthcare costs while, for instance, improving the quality of the healthcare system and reducing visits to emergency rooms and hospital stays [29].

To allow knowledge sharing and easy access among various healthcare stakeholders, medical records are stored on the cloud database being weighty [30]. Also, there are security and privacy measures accessible by cloud storage enhanced by data durability. In cloud storage, there is no interoperability between various healthcare providers and treatments. Moreover, it is not possible to guarantee the quality and authenticity of the data. To enhance the credibility, accuracy, and

authenticity of stored and shared medical information, blockchains play prominent roles. Blockchains guarantee the protection of sensitive data by monitoring access to confidential medical information and ensuring allowed access [30]. Against manipulation on harden medical information, blockchains act as a distributed database [31]. To addresses the safety concerns in IoT-based systems, blockchains used a distributed trust mechanism to distribute patient records on the cloud storage database that could be handled by various users and advisors like caregivers, physicians, clinic experts, pharmacies, patients themselves, and insurance providers.

To keep tracking past transactions related to the records of distributed patients, blockchains depend on hashing and public cryptography algorithms to maintaining confidentiality, integrity, and accessibility. This ensures that the documents are not destroyed, falsified, or accessed by unauthorized users. Patient records in blockchains may be appended to the database only, but not deleted. Using cryptographic hashing, new information can be securely connected to a previous record. Based on an agreement among the majority of miners in the blockchain, records are added to the blockchain. Miners are a group of special nodes that cooperate to verify new transactions added to a blockchain. Miners have to compete to solve a complex mathematical problem known as proof of work (POW), which takes an average of 10 min, to be able to add a record to a blockchain. This will help ensure that no one entity can alter or tamper with stored records that are checked. Furthermore, blockchains will enable caregivers to provide patients with encrypted alias targeted tailored health advice without the need to disclose their identities.

Blockchain technology is an incipient endeavor and must still be integrated with existing policies and processes, especially in the healthcare industry. The blockchain with related immutability, clarity, and distribution has been used by the National Research Council of Canada's Industrial Research Assistance Program (NRC-IRAP) to coordinate and disseminate public knowledge about its operations and companies, realizing that operating within government restrictions is a significant challenge all by itself [32]. The initiative achievement shows that public blockchain can be used to preserve government data, used to fix administrative obstacles, and potentially set a course for more complex data integration especially in smart healthcare [33]. The huge achievement of the projects creates a resourceful way to record meaningful information, exchange vital information, and act as an essential building block for potential more sensitive initiatives.

The distributed database management system (DDBMS) is technically centrally controlled (i.e., users fundamentally believe that a centralized database is running, but the underlying machines can be physically distributed), while blockchain is a peer-to-peer, decentralized database management system (i.e., each node runs independently while following the protocols) [34]. Blockchain is therefore ideal for applications where biomedical/healthcare stakeholders (e.g., hospitals, suppliers, patients, and payers) are independently controlled to communicate with each other without ceding power to a central management intermediary [35, 36].

In addition to patients' integrity and to maintain a precise timeline of events, IoT-based devices must be securely logged using commands given to actuator nodes as both records and the treatment for a patient must be approved by medical

experts. With this method, when it comes to wearing medical devices, providing an immutable ledger and automatic health incident updates in a safe manner would give patients peace of mind. The medical professionals get a real-time update concerning their patients, hence propagating the practice of precision medicine. The use of smart contacts helps in the automation of health alerts from various devices into centralized cloud storage, thereby creating a groundbreaking solution that allows healthcare providers to quickly leverage modern medical technologies.

## 4 Challenges of Blockchain in Smart Healthcare Systems

The implementation of blockchain technologies in healthcare is emerging and faced with major obstacles and big choices to make in the future. Regarding challenges in decade back, our social definition of privacy has grown, and blockchain technology may sustain at these borders with great potentials if adopted. If the choice is either implementing blockchain-based solutions or not, then the trade-off between the danger of information loss to privacy and in charge of one's data (supposing no major data leakages) should be considered. The new repositories created by cloud computing have given birth to big data; this might later be analyzed by AI to create a customized healthcare plan that can be used by physicians and policymakers.

If substandard and incorrect data is placed on the chain, the blockchain remains fair to its users; the chain will stay with low-quality and incorrect information since that is what can be trusted by immutability and decentralization [37, 38]. There are several new possibilities for blockchain and supporting technology, but attention must be drawn to the implementation process together with what came off knowledge [39, 40]. One of the interoperability solutions is vigilance regarding the information being processed, and provide answers to address inconsistencies and distribute confidence to various types of information. There is a new limited possibility in blockchain technology with the arrival of quantum computing and its anticipated capacity to break current encryption techniques [41]. It is not clear exactly when this will happen, but it seems to be likely within the next decade [27]. If the resistance of quantum computing to encryption is not fixed, then we would have several issues, because if the whole health data is stowed on publicly available servers in blockchains, then the stored information is at risk.

A key with a specific sequence of characters has the ability to access data in blockchain which can create an interesting problem; if a key is lost, then the information accessed by it becomes irretrievable. Then this becomes unfair just because if one of these keys is lost, the users lose access to a lifetime of health records. Then there have to be other methods or strategies that will be introduced to reconnect users with their data. These methods will now be replacing one question with another with existing solutions introducing back doors to accessing the blockchain's private data. The accessibility of more than one company to most servers is another problem in blockchain technology; if the decentralization of a blockchain is disrupted, then one agent will become the only consensus agent and

can change the blockchain keys, in contravention of the property of immutability. To protect against this eventuality, new technologies for consensus and government regulation around blockchain monopolization might be appropriate [27].

Blockchain technology aims to allow for the efficient exchange of information with stakeholders while maintaining the confidentiality of data and preserving the privacy of patients. This will encourage and give people the power to make healthy choices to enhance their health status around the globe. The world sees their data has been protected more than ever before using the blockchain model. What is now expected is a huge disruption of the healthcare sectors, beyond the hype, skeptics are worried about the complications, and many installed and invested parties are going to act against that transition, not to mention legal, legislative, and technological specifics that are yet to be found out.

If the complexities of standardization are continuously resolved, reliable privacy established protocols of anonymization are built, and the consensus is reached on the types of contracts required to manage information. Then this can bring about a new era of healthcare around the corner. However, these major problems mentioned above at this early stage have been substantial inroads be taking care of by the businesses established in the healthcare systems. With the use of AI, technology giants have already learned from data to show that the technology can generate important new insights with the huge data generated from the healthcare system, with an important central tenet being privacy and patient control. The sectors move toward the health singularity called a disruptive event in which personalized treatment is offered centered on a thoughtful understanding of each individual's system.

Transparency and confidentiality are other important challenges of using blockchain in healthcare sectors. Since "everyone can see everything on a blockchain network" [42, 43], increased openness and reduced secrecy, such as open data transparency during the transition, are commonly considered a blockchain limitation. The anonymized user using hash addresses can still be identified by analyzing and reviewing the publicly accessible transaction on the blockchain network, and thus only "pseudonymity" [44] is given by the blockchain network. Because of the patient-related information in healthcare applications, this system is important since health information protection is very critical.

The speed and scalability are some other challenges that are associated with patient medical information. The extensibility of blockchain-based applications can be limited by the protocol, transaction time, and speed. For example, because of the necessary computational workload, there are about 288,000 transactions per day or about 3.3 transactions per second on average for Bitcoin with the proof-of-work protocol, while a credit card such as Visa has an average of 150 million transactions per day or about 2000 transactions per second [45]. Because of the current protocol's 1-megabyte block size limit, Bitcoin's theoretical maximum transaction speed is 7 transactions per second, while Visa's theoretical maximum transaction speed is 4000 transactions per second [45]. This issue is critical when designing real-time and accessible blockchain-based affordable healthcare applications [35, 36]. In blockchain technology, in situations where patients do not have access to their

medical data, smart contracts are not feasible, for example, unconsciousness, drugs, dizziness, under the influence of alcohols, etc.

## 5 The Framework for a Secured Smart Healthcare Monitoring Systems Using Blockchain

The smart healthcare monitoring system is the medical-care-precise variant of IoT which could be introduced to deliver remedy or cure to healthcare professionals and guarantee quick and accurate diagnosis and treatment [46]. With the assistance of radars embedded in smart headsets, drones, robotics, and smart system self-sampling experiments, data collection may be performed. The purpose of smart healthcare systems has been sparked by the rising demand for remote patient management coupled with the storage capacity of the cloud. Well-implemented surveillance systems have caused the incidence of disease cases to be minimized, and their side effects [47]. The patient and warden make advice about the vital indications of their situation by multimedia due to the real-time function of patient monitoring [48]. Versatile, actual, and hetero connectivity provides a platform for a variety of innovations across the medical field to provide accessibility for participants [49].

This chapter proposes an intelligent secured smart healthcare monitoring system using blockchain for securing the IoT-based system on the cloud. The proposed system will overcome the challenges and issues encountered by the IoT-based system using various devices and sensors. The proposed system allows the use of a different range of wearable devices interconnected to monitor a person's health condition. The sensitive and private data of patient's EHR and health data captured through the wearable sensors were encrypted using the blockchain model, and are stowed in a dispersed cloud database rather than a central database.

The stored data on the cloud database can only be accessed by authorized users like caregivers, medical physicians and experts, pharmaceutical companies, healthcare insurance brokers, among others. The doctors or caregivers can only access patients' data and information if the said patient authorizes it since a notification will be sent to the patient that the data and information want to be accessed by a third party. The patient has to agree to share the data before a doctor or caregiver has access to such data and information. The entire system is connected with a wireless gateway, and the data were captured using Wearable Sensor Network (WSN). The design process of the secured monitoring system using blockchain technology is represented in Fig. 2.

The safety and confidentiality of records relating to patients are twofold essential notions. When we refer to record safety, this signifies that records are securely stowed and transmitted to ensure their absoluteness, genuineness, and legitimacy. Record confidentiality signifies that records can solitarily be obtained by individuals who are authorized to sight and utilize it [22, 23]. More rational security measures



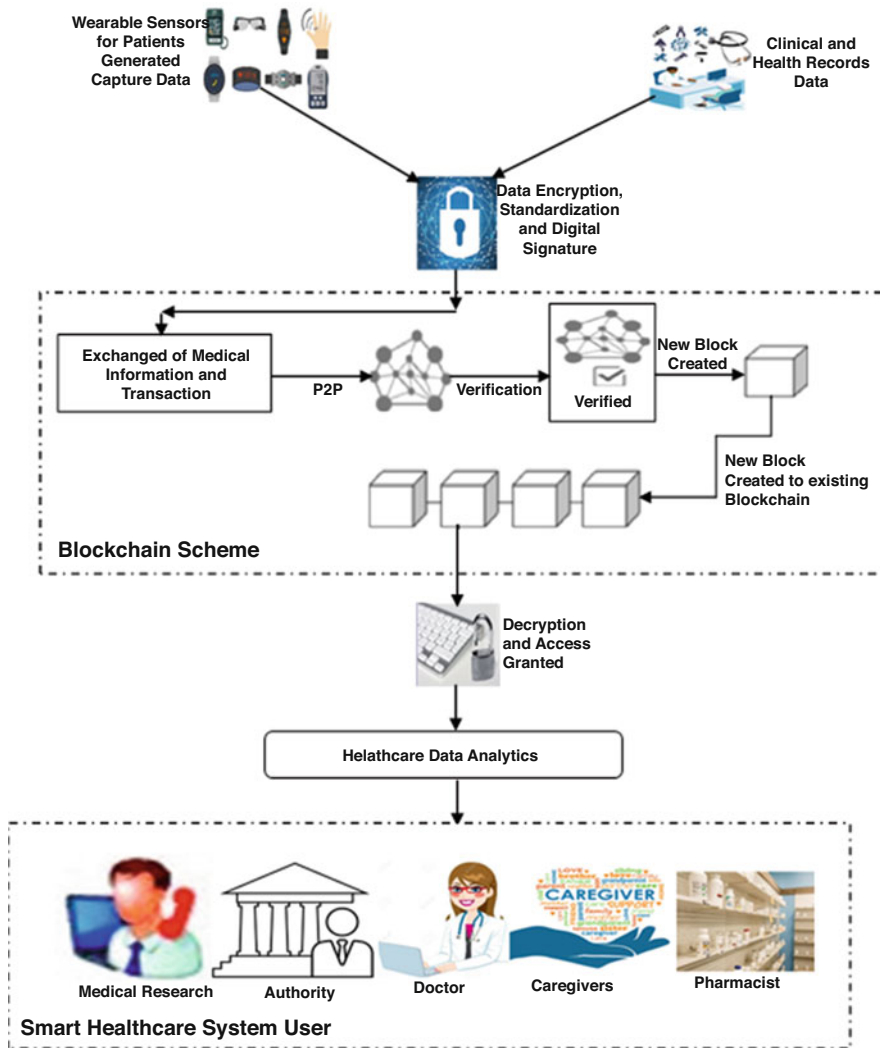


Fig. 2 The proposed blockchain smart healthcare monitoring system

may be established with different objectives and specifications in mind. The extensive utilization of IoT gadgets offers an improved assurance of an individual’s health [24], but it also places a great deal of demand on record safety and concealment.

Consequently, efficacious IoT advancement needs to accept safety and confidentiality as an essential concentration. Though most healthcare establishments don’t devote sufficient funds to shield safety and confidentiality [22, 50], there isn’t any hesitation that safety and confidentiality perform a significant function in IoT. IoT gadgets create a growing amount of ever more complex real-time records,



which is extremely delicate. On one side, the failure of health organizations or system security may have catastrophic consequences. On the other hand, privacy information for the patient is accessible at all levels of record processing, record transfer, cloud storage, and record republication. The framework consisted of five entities and the roles of each are described below.

**IoT-Based Wearable Devices** These instruments are used in real time to capture the patients' symptoms and proctor the conditions of patients. These devices consist of various sensors that detect the patient's atmosphere and vitality (like temperature, blood pressure, pulse rate, heart rate, humidity, ECG, etc.). The physicians and clinicians are alerted in real time when there is a deviation in these criteria (from the permitted limits). The short message services are used to report any case to the concerned physicians, and the message arrives on the smart devices.

**The Clinical Data/Medical Records** Continuous patient monitoring creates vast quantities of data. In real time, this data is not always useful, but when intelligently analyzed, it can provide valuable insights. The cloud database is used to store the information obtained by the smart wearable system and other tracking units. Before storing the data, the system encrypted the data so that any security breaches and data leakage can be avoided.

**Encryption/Decryption and Standardization** This layer is the top significance of the projected secured system. There are primarily diverse formats of data and information collected by various sensors. The medical information needs to be turned into a standard format to perform well-organized big data analytics. The role of encrypting data and information using the blockchain instrument is also carried out by this device. Under this, all the system's stakeholders are designing and digitally signing smart contracts. For an immutable structure, the blockchain has to prove fool with user privacy; it provides complete protection, continuity, and transparency.

**Blockchain Instrument** The transactional data gets stored building immutable storage blocks. The data is only permitted to be accessed by legitimate users. Blockchain technology enables us to build privacy-preserved and inherently protected data exchange networks that allow the participating agencies to easily access archived and real-time patient data using smart contracts that fully remove the overhead of data reconciliation. There is no single administrator in a traditional Blockchain; thus, there is a dispersed system of control and access with some level of interest in each participant, which all share equal rights and power.

**End Users** The patient uses the system through smart devices, and the medical experts interact with the system through the smartphone or web interface. That includes the patients, physicians, nurses, druggists, clinicians, pharmacists, insurance providers, and scholars.

Two-level blockchain techniques are used in the proposed framework. A private blockchain is used by the healthcare environment's internal agencies, such as treatment providers, physicians, inventory, and other internal stakeholders. To

communicate with external organizations such as patients, pharmacists, insurance providers, etc., a public blockchain is used. The use of the two-level implementation of blockchain provides separation between various entities and thus provides a secure and privacy-preserved, consistent, and transparent workflow.

The blockchain layer analyzed data collected from the overall status data from terminals in addition to the network traffic to identify responses to security breaks or coercions to the system. This was done to identify in real time some attack circumstances to device trends and set up countermeasures against such situations. This can be done using the intrusion activity pattern with an access control strategy from the gathered protection status data from the IoT-based environment. The analysis feature looks for events or patterns that may cause a particular device to have security vulnerabilities or threats. Malicious conduct analysis and rule-based analysis are performed at this level.

The malicious behavior analysis discovers abnormal activities by scrutinizing usage trends in the system after studying normal activities. The events that do not occur in a normal system were analyzed using rule-based and, according to the established rules, define security threats. In the case of a security incident, it analyzes intrusion actions and suggests countermeasures. Before a security attack happens, this feature prepares for security incidents by security policies. The identification and recovery of threats work to detect an existing safety incident and to restore the damage to normal status. In the event of an attack or security incident, the security forensics feature examines basic vulnerabilities and abuse cases.

Information exchange between terminals is supported by the communication layer, which includes a variety of radar gadgets and items that can be connected through a radio receiver connection. Wi-Fi, ultra-wideband, RFID, ZigBee, and Bluetooth could all use this radio receiver connection. The IoT gateway will bind to multiple networks and tolerates cyberspace. The upper level is about big data analytics, which involves processing large amounts of data collected from radars in the cloud and making it available to big data analytics users. These frameworks provide API tracking and a dashboard to help with engine contact management.

## **6 Conclusion and Future Directions**

The integration of computer and biomedical technologies in medical systems has supported healthcare events, for instance, real-time disease analysis, remote monitoring of patients, and real-time drug prescriptions, among others. The methods have significantly helped to store both patients' personal information and their symptoms on the cloud, which can help during contagious diseases. This aids the quality of services provided by the physicians, thereby improving patients' satisfaction. But there are still security and privacy challenges faced by the smart healthcare system, and many users are not ready to use the platform. The diversity of IoT components makes the security concerns of IoT applications more complex for users. Thus, it is the main concern for the production of these smart healthcare system applications to recognize and deal with these security problems. Therefore, this chapter proposed a

secured smart healthcare system using blockchain technology. The proposed system was used to turn the concentrated and fragile smart system into a distributed, transparent, and protected system, thus improving the standard of medical-related services on the smart healthcare system. There are several explanations regarding blockchain as a way of enhancing the healthcare system. First, it supplies clear data to all stakeholders while protecting the patients' privacy. Furthermore, it protects valued medical records from theft and snooping from vicious attackers. It also puts a check on the costly inefficiencies of the system. Blockchain-based healthcare networks will provide the end user like medical researchers, physicians, drug supply chain, and caregivers among others with affordable and safe services. Future work will look into the achieving scalability and flexibility of the smart healthcare system; the need for the designing of universal standards for the adoption of blockchain will be also looked into in future work. The full implementation of the proposed framework will be carried out in a future direction. The blockchain knowledge gap among the healthcare stakeholders is a major hurdle in its deployment which will be addressed in the future for adequate implantation of blockchain in the healthcare system.

## References

1. S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **5**, 26521–26544 (2017)
2. F. Fernandez, G.C. Pallis. Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective, in 2014 4th international conference on wireless Mobile communication and healthcare-transforming healthcare through innovations in Mobile and wireless technologies (MOBIHEALTH), pp. 263–266. IEEE 2014, November
3. J.S. Guy, Digital technology, digital culture, and the metric/nonmetric distinction. *Technol. Forecast. Soc. Chang.* **145**, 55–61 (2019)
4. G. Tripathi, M.A. Ahad, S. Paiva, S2HS-A blockchain-based approach for the smart healthcare system, in *Healthcare* vol. 8, no. 1 (Elsevier, 2020, March), p. 100391
5. J.B. Awotunde, R.O. Ogundokun, S. Misra, Cloud and IoMT-based big data analytics system during COVID-19 pandemic. *Internet of Things*, 181–201 (2021)
6. C.M. Medaglia, A. Serbanati, *An Overview of Privacy and Security Issues on the Internet of Things*, The Internet of Things (Springer, New York, 2010), pp. 389–395
7. P. Yang, W. Wu, M. Moniri, C.C. Chibelushi, Efficient object localization using sparsely distributed passive RFID tags. *IEEE Trans. Ind. Electron.* **60**(12), 5914–5924 (2012)
8. AL-Mawee, W. (2012). Privacy and Security Issues in IoT Healthcare Applications for Disabled Users a Survey
9. J.B. Awotunde, C. Chakraborty, A.E. Adeniyi, Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. *Wirel. Commun. Mob. Comput.*, 7154587 (2021)
10. J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, Y. Tang, Cloud-aided lightweight certificates authentication protocol with anonymity for wireless body area networks. *J. Netw. Comput. Appl.* **106**, 117–123 (2018)
11. S. Roy, S. Chatterjee, A.K. Das, S. Chattopadhyay, S. Kumari, M. Jo, Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowd-sourcing Internet of Things. *IEEE Internet Things J.* **5**(4), 2884–2895 (2017)

12. A.D. DeVore, J. Wosik, A.F. Hernandez, The future of wearables in heart failure patients. *JACC Heart Fail.* 7(11), 922–932 (2019)
13. Mack, H. (2017). The Remote Patient Monitoring Market Grew by 44 Percent in 2016, the Report Says
14. E.A. Adeniyi, R.O. Ogundokun, J.B. Awotunde, IoMT-based wearable body sensors network healthcare monitoring system, in *IoT in Healthcare and Ambient Assisted Living*, (Springer, Singapore, 2021), pp. 103–121
15. H. Tao, M.Z.A. Bhuiyan, A.N. Abdalla, M.M. Hassan, J.M. Zain, T. Hayajneh, Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet Things J.* 6(1), 410–420 (2018)
16. S.P. Amaraweera, M.N. Halgamuge, Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues, in *Security, Privacy, and Trust in the IoT Environment*, (Springer, Cham, 2019), pp. 153–179
17. M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient-centric agent: A block architecture. *IEEE Access* 6, 32700–32726 (2018)
18. O. Vermesan, P. Friess (eds.), *Internet of Things—from Research and Innovation to Market Deployment*, vol 29 (River Publishers, Aalborg, 2014)
19. J.B. Awotunde, R.G. Jimoh, S.O. Folorunso, E.A. Adeniyi, K.M. Abiodun, O.O. Banjo, Privacy and security concerns in IoT-based healthcare systems. *Internet of Things*, 105–134 (2021)
20. F. Alsubaei, A. Abuhusseini, & S. Shiva, Security and privacy on the internet of medical things: Taxonomy and risk assessment, in 2017 IEEE 42nd conference on local computer networks workshops (LCN workshops), pp. 112–120. IEEE, 2017, October
21. A.A. Mutlag, M.K.A. Ghani, N.A. Arunkumar, M.A. Mohammed, O. Mohd, Enabling technologies for fog computing in healthcare IoT systems. *Futur. Gener. Comput. Syst.* 90, 62–78 (2019)
22. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and privacy in the medical internet of things: A review. *Security Commun. Netw.* (2018)
23. J. Tang, A. Liu, M. Zhao, T. Wang, An aggregate signature-based trust routing for data gathering in sensor networks. *Security Commun. Netw.* (2018)
24. W. Sun, Z. Cai, F. Liu, S. Fang, G. Wang, A survey of data mining technology on electronic medical records, in 2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom), pp. 1–6. IEEE, 2017, October
25. O.C. Abikoye, U.A. Ojo, J.B. Awotunde, R.O. Ogundokun, A safe and secured iris template using steganography and cryptography. *Multimedia Tools Appl.* 79(31–32), 23483–23506 (2020)
26. F.E. Ayo, S.O. Folorunso, A.A. Abayomi-Alli, A.O. Adekunle, J.B. Awotunde, Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. *Information Security J.* 29(6), 267–283 (2020)
27. C. Chakraborty, B. Gupta, & S.K. Ghosh, Mobile telemedicine systems for remote patient’s chronic wound monitoring, in *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*. (IGI Global, 2020), pp. 977–1003
28. A. Banerjee, C. Chakraborty, A. Kumar, D. Biswas, Emerging trends in IoT and big data analytics for biomedical and health care technologies, in *Handbook of Data Science Approaches for Biomedical Engineering*, (Academic Press, 2020), pp. 121–152
29. C. Chakraborty, J.J. Rodrigues, A comprehensive review on device-to-device communication paradigm: Trends, challenges, and applications. *Wirel. Pers. Commun.* 114(1), 185–207 (2020)
30. Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J.A. Abedlla, K. Shuaib, Introducing blockchains for healthcare, in 2017 international conference on electrical and computing technologies and applications (ICECTA), pp. 1–4. IEEE, 2017, November
31. J.B. Awotunde, R.O. Ogundokun, S. Misra, E.A. Adeniyi, M.M. Sharma, Blockchain-based framework for secure transaction in mobile banking platform. *Advances in Intelligent Systems and Computing*, 525–534 (2021., 1375 AIST)

32. M. Mettler, Blockchain technology in healthcare: The revolution starts here, in 2016 IEEE 18th international conference on e-health networking, applications, and services (Healthcom), pp. 1–3. IEEE, 2016, September
33. C.B. Krubiner, D.A. Schwartz, Viral hemorrhagic fevers in pregnant women and the vaccine landscape: Comparisons between yellow fever, Ebola, and Lassa fever. *Curr. Tropical Med. Rep.* **6**(4), 186–196 (2019)
34. T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, ..., A. Granzotto, BigchainDB: a scalable blockchain database. White chapter, BigChainDB, 2016
35. L.A. Linn, M.B. Koo, *ONC/NIST Use of Blockchain for Healthcare and Research Workshop* (HealthIT. gov, Gaithersburg, 2016)
36. A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, *ONC/NIST Use of Blockchain for Healthcare and Research Workshop* (Gaithersburg, 2016)
37. S.A. Abeyratne, R.P. Monfared, Blockchain-ready manufacturing supply chain using a distributed ledger. *Int. J. Res. Eng. Technol.* **5**(9), 1–10 (2016)
38. N. Kshetri, 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **39**, 80–89 (2018)
39. A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On Blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Comput. Syst.* **88**, 173–190 (2018)
40. W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology* (Wiley, 2016)
41. D.J. Bernstein, N. Heninger, P. Lou, L. Valenta, Post-quantum RSA, in *International Workshop on Post-Quantum Cryptography*, (Springer, Cham, 2017, June), pp. 311–329
42. G. Greenspan, Multichain private Blockchain-white chapter. <http://www.multichain.com/download/MultiChain-White-Chapter.pdf>, 2015
43. P. De Filippi, The interplay between decentralization and privacy: The case of blockchain technologies. *J. Peer Prod.* **7** (2016)
44. M. Moser, The Anonymity of Bitcoin Transactions, 2013
45. T.T. Kuo, H.E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **24**(6), 1211–1220 (2017)
46. M. Abdulraheem, J.B. Awotunde, R.G. Jimoh, I.D. Oladipo, An efficient lightweight cryptographic algorithm for IoT security. *Commun. Comput. Information Sci.* **2021**(1350), 444–456 (2021)
47. A. Craven, M.M. Eloff, Biometrics as an Agent to Reduce Fraud in the Micro Lending Industry in South Africa, in ISSA, 2010
48. TRUSTe, TRUSTe Internet of Things privacy index—US edition, 2014
49. D. Kotz, K. Fu, C. Gunter, A. Rubin, Security for mobile and cloud frontiers in healthcare. *Commun. ACM* **58**(8), 21–23 (2015)
50. M. Huang, A. Liu, T. Wang, C. Huang, Green data gathering under delay differentiated services constraint for the internet of things. *Wirel. Commun. Mobile Comput.* **2018**(3), 1–23 (2018)

# Computational Intelligence in Healthcare with Special Emphasis on Bioinformatics and Internet of Medical Things



Siddharth Banyal , Deepanjali Mehra, Amartya, Siddhant Banyal ,  
Deepak Kumar Sharma , and Uttam Ghosh 

## 1 Introduction

Computational Intelligence (CI) is constantly burgeoning in diverse fields to encircle almost every facet of human interaction with a computer and providing numerous applications across all the fields in biomedical and bioinformatics. This chapter would aim to provide a comprehensible and concise understanding of Computational Intelligence-based schemes in the biomedical field, providing special emphasis on bioinformatics and the Internet of Medical Things (IoMT).

---

S. Banyal

Department of Information Technology, Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University, New Delhi, India

D. Mehra · S. Banyal

Department of Instrumentation and Control Engineering, Netaji Subhas University of Technology (formerly Netaji Subhas Institute of Technology), New Delhi, India

e-mail: [deepanjalim.ic.17@nsit.net.in](mailto:deepanjalim.ic.17@nsit.net.in)

Amartya

Department of Manufacturing Processes and Automation Engineering, Netaji Subhas University of Technology (formerly Netaji Subhas Institute of Technology), New Delhi, India

e-mail: [amartya.bt.17@nsit.net.in](mailto:amartya.bt.17@nsit.net.in)

D. K. Sharma (✉)

Department of Information Technology, Netaji Subhas University of Technology (formerly Netaji Subhas Institute of Technology), New Delhi, India

U. Ghosh

Vanderbilt University, Nashville, TN, USA

e-mail: [Ghosh.uttam@ieee.org](mailto:Ghosh.uttam@ieee.org)

## 1.1 Contemporaneous Work and Development of Intelligence in the Healthcare Industry

CI being a multifaceted discipline has completely revolutionized the field of biomedical and bioinformatics. CI subfields are being used to comprehend and resolve convoluted problems in the field of healthcare; these include fuzzy systems, artificial neural networks (ANNs), evolutionary computation, and swarm intelligence, as illustrated in Fig. 1.

The term Computational Intelligence aims to perform intelligent complex behavior by analyzing the adaptive mechanism and learning from the data. In a vernacular manner, the term CI means the cognitive ability of a computer to exhibit humanlike behavior. CI as a field is continuously evolving and plays an instrumental role in developing intelligent systems. Problems in biomedical engineering are now solved with the advent of CI-based techniques such as computer vision, speech processing, hybrid systems, neural networks, and expert systems. The challenge pertinent to high dimensionality could be removed by using feature selection techniques such as the filter method, wrapper method, and embedded method. The perpetual aim of CI approaches hinges upon analyzing and creating flexible processing of information such as assimilating, sensing, and recognizing. With the profusion of data comes a myriad of opportunities for the development of intelligent systems. As a result, CI presents innovative and promising new opportunities in the field of healthcare systems. Currently, smartphones have tangibly overpowered the people, relying more on technology; the future of optimizing healthcare with the aid of CI is ripening. The advent of CI in the area of biomedical imaging

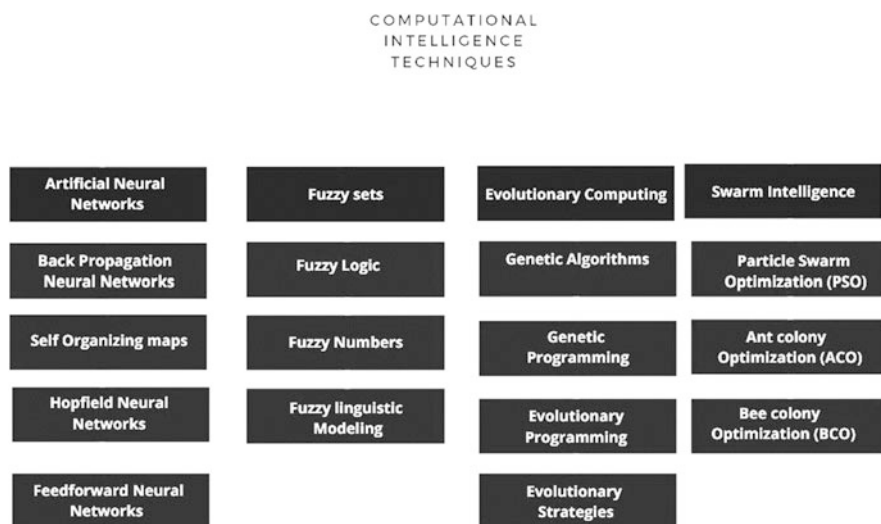


Fig. 1 Computational Intelligence techniques

is a key technique of computer-aided diagnosis (CAD) systems. CI uses heuristic models and algorithms based on geometrical, statistical, physical, functional, etc., and then use image datasets to provide an efficient method to devise models that can compute final classification labels from a stock of medical images. Magnetic resonance imaging (MRI) is an application of digital image processing in the detection and removal of a brain tumor [1]. Issues such as the high resolution of medical images and small datasets increase the computational costs, an area of concern. Clinical Data Warehouse (CWD) is accentuating research avenues in the healthcare field and also resolves the issue of limited datasets [2]. The advent of modern AI in medical and healthcare can be traced back to 1960. Cohen Moses used a supervised learning approach for the diagnosis of bacterial infections in patients with liver disorders [3]. The study conducted by Deedwania who devised exercise test predictors for patients suffering from ischemia concluded the risk of the disease could be precisely recognized using selected exercise parameters [4]. A plethora of intelligent systems was developed in the field of healthcare. In the last two decades, probabilistic graphical models such as Bayesian networks (BNs) have been increasingly correlated in the field of cancer research specific to medical diagnosis [5]. There are three cognitive approaches for developing, and they are Bayesian networks, expert-driven, data-driven, and hybrid Bayesian networks. Bayesian networks addressed a myriad of issues such as prognosis of breast cancer, liver disorder, diabetes, etc.

The term Internet of Medical Things (IoMT) is recently coined with the advancements in the medical field. The data is procured from a myriad of devices including sensors and other biomedical systems which are then analyzed using statistical modeling techniques. With the rise of IoMT, along with smart devices, there is an increasing demand for personal healthcare applications and providing effective solutions for diseases such as diabetic foot ulcers (DFU) [6]. Contagious diseases such as onychomycosis are now being treated with the aid of wearable devices that use ergonomic experiments [7]. Chien-Nan-Lee proposed wearable devices for Parkinson's disease [8]. The devices composed of a single-chip microcomputer procure plantar pressure and posture sway data and then convert it into statistical charts for distinguishing between normal gait and Parkinsonian gait.

## ***1.2 Overview of Computational Intelligence-Based Paradigms***

### **1.2.1 Artificial Neural Network**

Machines traditionally used either a functional or object-oriented basis. The code was written and extracted information in a predetermined manner. These standard algorithms had various shortcomings such as dealing with incomplete data, efficiency, error analysis, and limited functionality. The term artificial neural network was coined in 1958 by Frank Rosenblatt who developed a simple classifier; the model perceptron showed the processing of visual data by the human brain and



learned to recognize objects. For the past few years, there has been significant growth in the field of neural networks.

The paradigm of ANN is a convoluted system of interconnected networks of processing elements that draw inspiration from the functionality of the human cortex and aims to solve a particular problem [9]. Each processing element is called a neuron which is connected via synapses that have a particular weight value associated with it. These neurons are closely knit together and organized into different layers. In the input layer, the data is fed, the hidden layer is an intermediate layer for the processing of data, and the output layer gives the final answer. These neurons interact with each other through connected links and have the ability to store knowledge that is accreted from a learning process. Due to the complex interconnection of neurons, it is impossible to know the exact flow of data. ANN could be considered as a framework that learns, trains, and establishes a pattern among the data. It can efficiently process large amounts of data due to its parallel architecture. The basic building block of ANN can be analogous to that of biological neurons. The basic elements of a neural network constitute of:

- Synapses: This is a complex connection between neurons that plays a crucial role in neuron computation allowing the signal to pass from one neuron to another with each synapse associated with a distinctive neuronic value called trigger or weight values. These weight values are subjected to mathematical calculations, and the result is then multiplied by weight as it propagates further.
- Adder: It is a confluence point of all the input signals associated with weight values that are further summed up and fed to the activation function.
- Activation function: A nonlinear modification of input is done by taking into account the interaction effect with different parameters by activation function before evincing and finalizing the output. After the transformation process, activation function also called the squashing function decides an activation state of a neuron (on or off). There are various types of activation functions such as step function, sigmoid function, ReLU, tanH, etc.

The framework of an activation function might be influenced by the type of neural networks it wishes to serve and the nature of the algorithm it uses. Activation function if not applied generates a linear function (one-degree polynomial) that has less strength and finite complexity and hence will be inept to comprehend and model complex data such as speech, pictures, audio, etc.

### 1.2.2 Fuzzy Systems

In the traditional logic block, the computer produces an output of definite *true* or *false* upon taking a set of inputs which somewhat does not resonate with human reasoning of definite yes or no. Fuzzy systems are referred to as nonstatistical uncertainty closely resembling the real-world problems that do not have a definite answer of yes or no (1 or 0). CI provides us the flexibility to address these reasoning problems by presenting an intermediate value between 0 and 1. The fuzzy system

invented by Lotfi Zadeh provides acceptable reasoning and observed a range of possibilities such as (1) certainly yes, (2) possibly yes, (3) cannot say, (4) possibly no, and (5) certainly no, which helps in dealing with uncertainty in engineering. The architecture of fuzzy systems constitutes of four parts:

- **Rule base:** Based on linguistic information, it contains a pool of if-then inference rules that are rendered by experts to control the decision-making. Effective decision-making methods are devised for the design and tuning of the fuzzy controller that reduces the number of fuzzy rules significantly.
- **Fuzzification:** This block converts the crisp numbers into fuzzy sets that are measured from sensors and further are fed into control systems for further processing.
- **Inference engine:** It checks the degree of similarity among fuzzy inputs and rules and according to the input field and decides which rules are deemed to be fired.
- **Defuzzification:** Fuzzy sets are converted into crisp values by the process of defuzzification. Center of area, first of maxima, and mean of maxima are different forms of defuzzification techniques that aim to reduce an error of a specific expert system.
- The most frequently used fuzzy systems are the Mamdani fuzzy model, Tsukamoto fuzzy model, and Sugeno fuzzy model. There are myriad applications of fuzzy systems such as in the field of aerospace, chemical industry, automotive industry, and the biomedical industry.

### 1.2.3 Evolutionary Computing

Evolutionary computing uses stochastic search methods, a subfield of CI that draws its inspiration from biological evolution and hinges upon the idea of survival of the fittest by Charles Darwin to solve computational problems. Hence a system must have an adaptive approach for such computational problems so that it continues to function efficiently in a dynamic environment. The term evolution can be viewed as changes in the genetic attributes of a living being over a period of time. Evolutionary computing remains an active area of research that uses a bottom-up paradigm in which simple rules are formulated for the systems showing complex behavior to adapt. Features like mutation, inheritance, competition, and survival are the basic building blocks of an evolutionary algorithm (EA). In position to the neural network that uses a connectionist model, evolutionary algorithms (EA) use stochastic search methods that are inspired by Charles Darwin's model. During the period of the 1950s and the 1960s, various evolutionary computation methods were invented by scientists working independently. A myriad of evolutionary strategies was introduced that took real-valued parameters, selecting various features to be optimized. It aims to solve hard problems by evaluating multipoints simultaneously and carrying out an extensive probe over a large intermittent, convoluted, and non-differentiable surface.

Genetic algorithm (GA) invented by Holland in the early 1970s is the most widely used form of evolutionary algorithms that successfully covers a wide variety of real-world problems such as sequence optimization or learning tasks. The first step of the GA starts with the generation of the initial population which is composed of stochastically chosen individuals associating with search space. The population  $x$  is assigned at the beginning which then enters into a loop performing the following steps with each process being termed as generations: (1) evaluating strings and assigning them fitness value to each chromosome, (2) process of selection, and (3) variation which is performed where the application of three genetic operators, namely, selection, mutation, and the crossover, is done. The termination process occurs when the algorithm reaches maximum runtime or the algorithm has achieved some threshold level in terms of performance. Genetic programming, particle swarm optimization, evolutionary programming, etc. are some evolutionary computing algorithms. The real-world application of evolutionary computing includes data mining, fault diagnosis, classification, clustering, etc.

#### **1.2.4 Swarm Intelligence**

Swarm intelligence that aims to design efficient optimization and clustering algorithms took its inspiration from the biological collective behavior of species such as ants, swarm, bees, wasp, etc. These decentralized and self-organized agents are together referred to as colonies and tend to work on the principle of combination of many minds as a whole unit that aims to solve complex problems using an optimal approach. The characterizing attribute of a swarm is to act in a collective, coordinated, robust, and flexible manner without the need for an external controller. It can be observed by the biological nature of swarm that shows collective behavior without any intrusion from an external controller. These groups of swarm exhibit intelligent behavior by spatially interacting with neighboring individuals based on simple rules. Swarm intelligence systems are scalable which means they can increase their size while maintaining their function because it involves interaction among neighboring individuals due to which the number of interactions does not tend to grow with overall individuals in the swarm, hence increasing its performance, without the need for any reprogramming. Due to the decentralized and self-organized nature of their control structure, they have high fault tolerance. Swarm intelligence systems are sensitive, i.e., a different group-level behavior could be observed by even a small change in simple rules; also sometimes it becomes difficult to predict the behavior.

Particle swarm optimization (PSO) is a stochastic optimization approach that is a population-based search methodology in which every individual is referred to as a particle that is altogether grouped into a swarm that interacts locally with each other and environment. A predefined fitness function is used to measure the performance metric of each particle. River formation dynamics (RFD) algorithm is a metaheuristic optimization algorithm that takes its inspiration from how water forms a river and follows the mechanisms of erosion and soil sedimentation. RFD

is gradient oriented that aims to find the optimal solution by creating a set of agent droplets that performs an extensive search by traversing between nodes according to the decreasing gradient of nodes. Swarm intelligence proves a better solution due to its property of randomness that enables continuous exploration of alternatives and can be applied to a myriad of fields in fundamental research, engineering, and social sciences. Application of SI is the field of behavioral animation, distributive perceptive networks, robotics, library materials acquisitions, biomedical, etc.

### 1.2.5 Machine Learning Paradigms

Machine learning is a domain of AI that provides machines the cognitive ability to learn and make successful and accurate predictions without being explicitly programmed. Machine learning algorithms are capable of making decisions, generate a mathematical prototype from sample data, and make an accurate prediction by learning from previous computations. It involves continuously feeding the data to the machine so that it can interpret the data, detect patterns, and understand key features to solve complex problems. The history of machine learning could be traced back to the year of the 1950s when Alan Turing created a Turing test. Then in the year 1952, Arthur Samuel devoted a computer program that could learn to play checkers as it ran. Since then machine learning as a field has progressed a lot with increasing accuracy rate and continuous adaptive learning. Shedding more light on machine learning algorithm, Tom Mitchell in 1997 stated: “A computer program is said to learn from experience  $E$  with respect to some task  $T$  and some performance measure  $P$ , if its performance on  $T$ , as measured by  $P$ , improves with experience  $E$ ” [10]. Machine learning algorithms have been reliably discriminating between images, audio, video, etc. by being trained over a large amount of data. The end goal of machine learning algorithms is to enable automatic learning from a dataset through the process of training without any or minimal human intervention. Machine learning algorithms are often classified into three categories: supervised learning, unsupervised learning, and reinforcement learning:

- **Supervised learning:** Speaking in a vernacular manner the term supervised means to oversee or direct certain activities to make sure that it is done correctly; hence in this type of learning, our machines learn under guidance. In supervised learning, the mapping of input is done to the output based on a learning algorithm. During the training phase for supervised learning, it is imperative for a system to be exposed to a large amount of labeled data so that it analyzes the dataset, recognizes clusters, and masters the task given. After the training phase, new inputs are fed to get the output that is based on what the system has learned until now. The process of learning continues to perpetuate until the algorithm reaches an adequate level of performance.
- **Unsupervised learning:** Unsupervised machine learning algorithms learn information from uncategorized and unlabelled data without any supervision or guidance. In unsupervised learning, there is input data ( $x$ ) that has no parallel

output ( $y$ ). The algorithm groups the unstructured data analyzing and detecting patterns without the dataset being trained. In contrast to the methodology of supervised learning in unsupervised learning, there is no guidance or supervisor, and the algorithm explores the data and draws its inferences from the dataset rendering hidden structures from uncategorized data. Unsupervised learning uses clustering for the exploration of data and dimensionality reduction that makes the data digestible. In the field of bioinformatics, sequence analysis and genetic clustering are done using unsupervised learning methods.

- **Reinforcement learning:** Reinforcement learning is based on the system of action and rewards where agents interact with the environment making a sequence of decisions and producing actions that discover errors or rewards. The main aim of the system agents is to maximize rewards. Reinforcement learning can be thought of as a game situation where the system learns by trial and error approach, hence adjusting parameters and forming rules that will give the system reward.

### ***1.3 Potential of Computational Intelligence in Medicine and Bioinformatics***

CI holds a huge potential in the multidimensional field of medicine and bioinformatics as it possesses the ability to detect meaningful relationships to diseases diagnosis and treatment and truly reconfigure the healthcare industry. The production of antibiotics is one of the best-known examples in the field of medical biotechnology which is used to treat various bacterial infections. Cutting-edge technology is used to treat cancer cells using gene therapy (immunotherapy, oncolytic virotherapy, and gene transfer) that promises innovative treatment of diseases such as mesothelioma, hemophilia, severe combined immune deficiency (ADA-SCID), etc. Electroencephalogram (EEG) is a test that evaluates special types of brain disorders (such as brain tumor, epilepsy, dementia, stroke, encephalopathy) by detecting abnormalities in the electrical activity of the brain and is also one of the emerging trends.

For the past few years, big data has become a topic of special interest and is being increasingly used in the field of medicine and bioinformatics research. With the advent of digitization of records, large volumes of medical data are being generated from a myriad of sources such as clinics, patient records, and IoMT devices; it is imperative to derive meaningful knowledge through comprehensive analysis and requires efficient management of data. Electronic health record (EHR) that aims to stock data accurately includes patient's records such as medical history, prescriptions allergies, etc. in which data could be shared through a connected network or an interface. It helps in meeting the patient's privacy concerns by addressing the security aspect of data. The advent of bioinformatics started in the 1980s with sequence analysis of DNA and was considered storing and analyzing biomolecular data, but with recent emerging avenues in the field of CI and personalized medicine, it is now considered a much broader discipline. Bioinformatics combines high-

performance computing and information science to analyze and interpret biological data. Genomic medicine has significant prospective bestowing neoteric diagnostic and therapeutic solutions for patients having a complicated disorder. Genome sequencing is being used for comprehending and analyzing novel diseases such as SARS-CoV-2 (COVID-19) [11].

## 2 Challenges to Integration of Computational Intelligence in Medical Applications

CI as a field is constantly burgeoning and providing various medical organizations with its benefit, but there is a myriad of challenges such as data labeling, security issues, integration challenges, etc. that is illustrated in Fig. 2 appended below. As CI has become an intrinsic part of our daily lives, these sets of challenges need to be addressed and overcome to unlock its true potential and transformation capabilities.

### 2.1 Clinical Applicability of CI-Based Metrics

Clinical applicability has plagued the community and been an impending endeavor for Computational Intelligence researchers from an applicability perspective. This “chasm” of AI becomes evident when we weigh in efficacy from a clinical point and compare it with accuracy. The area under operating characteristics of a receiver is not best reflective of clinical applicability despite the prevalence of

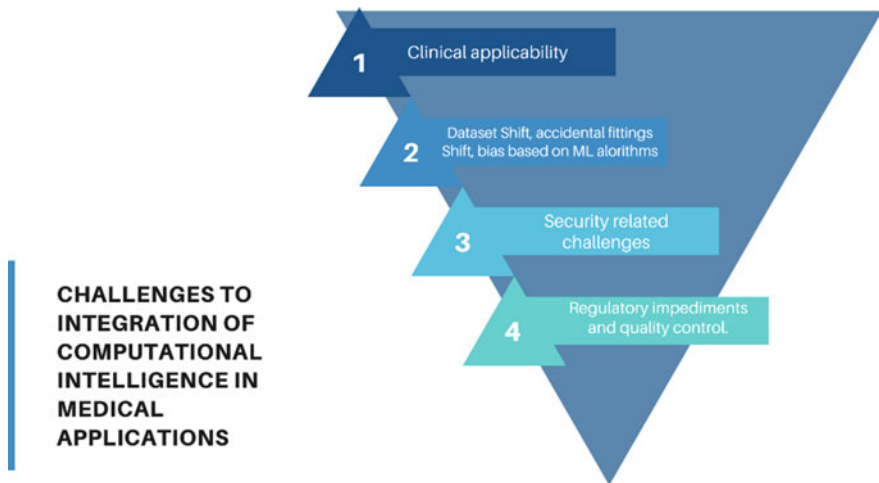


Fig. 2 Challenges in Computational Intelligence

machine learning-based research and also perplexes clinical experts. In addition to demonstrating sensitivity and specificity around a particular point of operation, the research studies often lack details of positive and negative values of predictions. A confluence of metrics is often used to summarize a model from a performance perspective as a single metric fails to do so. Even then these metrics fail to address things that are pivotal to patients such as insights on model results that can be used to change patient care.

This is vital as clinical experts need insights on how the CI-based algorithms could ameliorate care of patients under the ambit of a realistic workflow, something that also is missing from papers in this field. The works should also entail a cost-benefit and decision curve analysis that quantitatively assesses the benefit of a particular clinical action. This is possible if the gap between medical researchers and CI is bridged and cross-department collaboration and peer-reviewed studies are undertaken to critically appraise and adopt AI-based tools in this field.

## ***2.2 Machine Learning Challenges in the Medical Field***

### **2.2.1 Dataset Shift**

The term dataset shift also referred to as concept drift is a problematic situation in predictive modeling that occurs when the joint distribution of inputs and outputs differs between the training and test stages due to which the trained model won't provide the desired or the predicted results on the target dataset. It is to stress that if training and test distributions differ arbitrarily, then learning is not possible. The problem of dataset shift can stem due to a myriad of reasons such as data sparsity, selection bias/techniques approach of training and test sets, and the data distribution due to nonstationary environments that directly question the skill set of a data scientist. In the biomedical field, dataset shifts can be seen in image classification techniques such as magnetic resonance imaging (MRI) for diagnosing breast cancer, brain tumor, congenital heart disease, etc. Particularly in novel EHR algorithms where input data is generated within a nonstationary environment with a population of patients continuously changing (distributions of inputs changing) remains a great challenge. Dataset shift can be identified using techniques such as statistical distance (that identifies covariate shift), novelty detection, and the discriminative distance method. Feature removal is a method that is deployed to the correct dataset shift by setting a boundary; for a considerable level of shift, above a threshold value would be considered as a dataset shift. Features that are most responsible for the dataset shift can be removed from the dataset through an ablation study.

### **2.2.2 Accidental Fittings**

Machine learning algorithms are nothing but an evolution of regular algorithms that can review large volumes of data and analyze trends with the aim of increased efficiency and accuracy. Sometimes algorithms aiming to increase their efficiency tend to exploit certain confounding factors that have a counterproductive effect. Corroborating the above statement is an example that addresses grading in apples and allocates them, classes, using pixel-based artificial neural networks. It fails to allocate the proper grading in the apple when the stem end is inside the apple resulting in incorrect detections and has a counterproductive effect [12]. Similarly, in healthcare, there are similar concerns. A study conducted by Andre Esteva was more inclined to classify a skin lesion as virulent if the image had a ruler due to the fact of a ruler correlated function being present having an increased risk of a carcinogenic lesion [13].

### **2.2.3 Bias Based on ML Algorithms**

The term bias was first coined in 1980 by Tom Mitchell. Machine learning bias or algorithm bias is a phenomenon when improper conclusions about datasets or systematically prejudiced results are observed due to erroneous assumptions. Removal of deleterious bias embedded in the medical field where the diagnosis of the medical disease is a challenge needs to be addressed and requires extensive cognitive assessment to mitigate its effect. Factors such as race, gender, and economic background can be given an unfair bias and can ultimately lay out disadvantages to those present on the other side of the spectrum. For example, melanoma, a carcinogenic skin cancer, gives a bias to factors such as race/ethnicity for the prognosis of survival rates [14].

## ***2.3 Susceptibility to Attacks and Other Security-Related Challenges***

The field of biomedicine has vastly benefited with the advent of electronic health records (EHR) which bestows many advantages such as reduced medical errors, effective diagnosis, improved decision-making, making patient-physician communication better, etc. But it opens a window for hackers for security breaches, system intrusions, security attacks, and phishing attacks. There is a need for data governance for the efficient management of data and increased data security and privacy. These issues could be resolved using solutions adopting HIPAA compliance that improves the overall security and facilitates data access and data control. Web filtering techniques such as rating, keyword matching, blacklisting, and dynamic filtering can be deployed to deal with data losses and protect against exploit kits but



are prone to errors like false positive and false negative [15]. Effective anti-spam filters can act as the first line of defense against hacking attacks and phishing scams that can significantly improve security. Cryptographic hardware deploys a secure framework that stores the data in an encrypted format to improve data management and security and eliminate the need for storing biomedical data by a third party.

## ***2.4 Regulatory Impediments and Quality Control***

An appropriate regulatory framework is a rudimentary component to effectuate a safe and effective deployment of AI algorithms. This lays out unique concerns considering the current rate of innovation, dynamic nature of ML algorithms, and consequential risk associated. There is a need for effective regulations that will instill confidence in patients and healthcare professionals. With different regulatory bodies working on defining new regulations, the US Food and Drug Administration guidance is in the process of developing a state-of-the-art regulatory framework that will ensure that safe and effective technology reaches the patients.

Often this comes as a double-edged sword when protectionist regulations impede smooth approval of experimental trials or product introduction which deters the development of such CI-enhanced medical procedures or products. Hence a strong emphasis on cutting red-tape procedures is required from a public-policy perspective that while observing safety does not impede the introduction of CI-based paradigms in clinics.

## **3 Computational Intelligence in Biomedical Engineering**

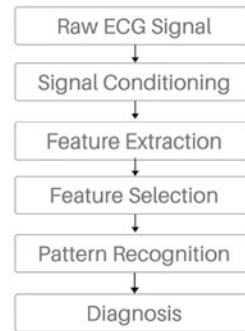
Computational Intelligence has found varied applications in diverse biomedical and healthcare. This section explains some of the most important areas such as cardiology, analysis of electromyography and electroencephalogram signals, and gait and movement patterns.

### ***3.1 CI in Cardiovascular Disease Diagnosis***

As per the World Health Organization (WHO), cardiovascular diseases (CVDs) are one of the foremost causes of death all over the globe which claims nearly 17.9 million lives every year. Despite the massive number of lives CVDs claim each year, there exists an extreme shortage of methodologies and mechanisms which can help track and monitor the forthcoming disorders based on behavioral patterns for early-stage diagnosis, counseling, and management. With the growing use of CI in the healthcare industry, the problem of early-stage diagnosis can be easily curbed

**Fig. 3** ECG signal processing description

## ECG SIGNAL PROCESSING



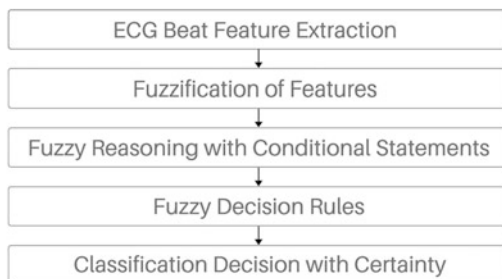
using ECG recordings and other diagnostic test data. ANNs are one of the most widely used techniques for ECG diagnosis, and one of the foremost applications was beat detection in ECG readings due to the ease of multilayer perceptron application. Using the backpropagation algorithm in MLP, arrhythmias were first classified. Early studies harnessed MLP to distinguish ventricular heartbeats from normal heartbeats. Similarly, using NN ECG classifiers, Marques et al. were able to detect ventricular hypertrophies and myocardial infarcts from normal rhythms with an accuracy of more than 80%. Figure 3 provides a basic description of ECG signal processing.

Neural networks have also been harnessed for analysis of ECG recordings like obtaining separate ECG of the fetus from the integrated ECG of both mother and the fetus by using an adaptive linear network (ADALINE). Like adaptive filtering techniques, in the ADALINE approach, NN can emulate signals from the mother closely and then discern the ECG component of the mother from combined ECG. Support vector machines work similarly to ANNs, the only difference of its applications to smaller datasets. Furthermore, two new algorithms on differential diagnosis rooted in the onset criterion of ventricular EGM were propounded. Genetic algorithms (GA) and SVMs are used together to classify unstable angina using Gaussian kernel to achieve a prediction rate as high as 79% with negligible false positivity. SVM's applications include arrhythmia detection algorithms, which were further improved by including endocardial ECG as well.

Using hidden Markov models, it was found that including P wave information of an ECG which corresponds to ventricular diastole is critical for the detection of supraventricular arrhythmias and can only be done by remodeling the ECG waveform as a single parametric model using HMMs. Doing so improved the classification accuracy by up to 97%. This approach has since been used to beat segmentation and ECG classification [16]. Similarly, fuzzy logic and fuzzy methods have been applied for the recognition of ECG signals. These approaches are equally viable for the classification of arrhythmia based on a system that assesses the QRS complex and P wave shape of the ECG wave signal. It is observed that the fuzzy

**Fig. 4** Fuzzy system for diagnosis and detection of CVDs using ECG signals

## FUZZY SYSTEM FOR DETECTION OF CARDIOVASCULAR DISEASES USING ECG



methods used are highly effective in granularity and also provided methods to tackle problems of incomplete input data as compared to other classification mechanisms. Similarly, C4.5 classifiers and the instance-based algorithm have also been used for the recognition and classification of heart-related diseases with an accuracy of 74.8%. Another study showed that the development of another classifier which is a fusion of k-nearest neighbor and naive Bayes classifier was used on the heart disease dataset and was able to process the accuracy of 82.96% [17].

The success of these technologies independently led to the development of hybrid systems that used multiple classifiers simultaneously. These hybrid systems or expert systems as they called were initially designed for beat recognition for diagnosis for cardiovascular diseases. As [18] developed a system that used SVM classifiers as base classifiers, which identified high-order statistical features and Hermite functions from ECG waveforms using the MIT-BIH database into 13 different beat types. Further, these systems have been used to create an entire knowledge base for coronary care but have faced challenges like design, maintenance, and collection of such large databases. Figure 4 depicts the mechanism involved in the classification of cardiovascular diseases using fuzzy logic.

### 3.2 CI in the Analysis of Electromyography Signals

The human body can perform various activities with the help of a neuromuscular system which comprises two different systems working in tandem, namely, the nervous system and musculoskeletal system. They are used for generating moments and forces by contraction or relaxation of muscle fibers to perform required actions. Therefore, unlike the cardiovascular system where the heart is the sole chief organ responsible for the entire system, the entire neuromuscular system is susceptible to diseases such as the different muscle groups, nervous system, and their junctions. Therefore, it becomes a difficult task to diagnose disorders especially if different

disorders involving different sections of the neuromuscular pathway display similar features.

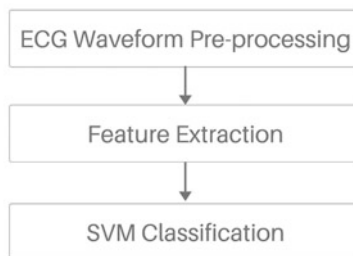
In electromyography signals, cell action potential and waveform are used for monitoring neuromuscular states during muscle activity and location and type of disorder. The use of CI techniques to diagnose and classify EMG signals and waveforms for reduces the burden on specialists and fastens the process of administering the treatment of disorder at the early stages. These methods generally operate by preprocessing EMG signals and then analyzing distinguishing characteristics such as time and frequency domain information, wavelet coefficients, and autoregressive coefficients, which are then used for classifiers such as neural networks or support vector machines to categorize diseases and identify muscle activity. However, with the difference in amplitudes and duration of electrical cell potential, which varies with age and gender, therefore, it becomes important to preserve distinguishing features that can be used for classification.

The discussion of CI techniques discussed in this section includes classifiers such as ANNs, SVMs, and fuzzy logic. The early uses of ANN classifiers to classify the cell action potential of muscle groups yielded results with nearly 85% accuracy. Further, this research was expanded by using K-means, MLP-NN, SOMs, and genetic-based classifiers. Using the abovementioned classifiers, it was found that NN and genetic-based models have better results. NNs are actively being used for the classification of neuromuscular disorders online. There were nearly ten characteristics described, which were identified, and characteristic selection used along with NN gave results with a classification accuracy of 95%. The SVMs were later used after NNs for diagnosis and classification to improve the accuracy provided by NNs. Xie et al. used multiclass SVM classifiers to identify and differentiate between healthy subjects and neuromuscular disorder patients [19]. The classifier was able to elicit attributes like spike amplitude, duration, and frequency of turns. The multiclass SVM classifier was able to classify patients with a precision of greater than 80% as compared to the MLP network, which was able to achieve an accuracy of nearly 75%.

Generally, fuzzy logic techniques are used along with NN classifiers such as the one proposed by Xie et al. [20], which utilizes fuzzy integral coupled with different NNs using time-domain measure, AR, and cepstral coefficient input data. The results from the hybrid fuzzy system yielded better results of nearly 88% accuracy as compared to the NN classifier used for single characteristics. Medical decision systems have been developed which rely on fuzzy Logic and measures and probabilistic rules. Suojanen et al. used causal probabilistic networks to determine the key attributes of diagnostic processes. For diagnostic purposes, the diagnosis was segmented into multiple phases with each phase being used to narrow down the search for possible diseases starting from considering single diseases followed by a pair-wise comparison of diseases for elimination. This method was first used for neuromuscular disorders. This method had a significant impact since it reduced computational time without reducing computational accuracy. Furthermore, fuzzy logic is being developed for helping in biomedical systems such as the delivery of muscle relaxants as general anesthesia during a surgical operation to control the

**Fig. 5** Supply vector machine classification mechanism

## SUPPLY VECTOR MACHINE (SVM) CLASSIFICATION MECHANISM



system with the use of neuro-fuzzy controllers. Figure 5 shows the flow diagram of classification mechanisms of data using SVM classifiers.

### 3.3 *CI in the Analysis of Electroencephalogram Signals*

The brain activity of a person is not only important just to monitor and diagnose neuromuscular disorders, but it is also used for early detection of neurological diseases such as epilepsy; for this, an electroencephalogram is used. This is done by placing electrodes on the scalp to detect electrical signals generated by neurons in the brain. While recording electroencephalogram signals, it has been observed that noise from the environment and the equipment used is also generated. Out of all the neurological disorders, epilepsy is one of the topmost neurological disorders affecting nearly 50 million humans globally. Epilepsy, which is caused by excessive brain electrical discharge and leads to seizures, is generally diagnosed using electroencephalogram signals. These signals, when processed using CI classifiers, are used to identify and distinguish between healthy EEG signals and seizure-affected individuals. The EEG signals of a person suffering from such a disorder have certain key patterns, which are called “repetitive high-amplitude activities” which are depicted by rapid, slow, or an amalgamation of spikes and slow waves. Generally, identifying the EEG signal activity of healthy or non-epileptic individuals from epileptic individuals is a time-inefficient and cumbersome process. Therefore, with the use of artificial neural networks, classifiers along with feature selection algorithms applied to EEG signals were able to achieve an accuracy of approximately 86% [21]. Furthermore, other techniques like fuzzy clustering and hybrid techniques are also being developed for analysis and classification. In 1998, Geva and Keram et al. performed EEG identification techniques on rats by using the unsupervised optimal fuzzy clustering algorithm. The inputs obtained from the EEG signals before and during epilepsy seizures by applying wavelet transform methods were used to classify and identify seizure events. Multiple classifiers to identify

epilepsy events have also been used and are called hybrid approaches. This was done by a fuzzy logic technique along with genetic algorithms (GA) to optimize EEG output signals. For determining the input risk factor, information regarding energy, spike waves, duration, events, and covariance measurements into binary and continuous GA. This process was observed to yield an accuracy of over 90% in identifying epilepsy events [22].

CI techniques have been applied to various other diseases, as well as Huntington's disease (HD) and Alzheimer's disease (AD). Huntington's disease is a genetically inherited disease that causes cell death in certain regions of the brain such that it causes psychiatric, cognitive, and physical abnormalities in children. With the help of EEG signals, it has been found that Huntington's disease causes a substantial loss in alpha rhythm. Furthermore, when EEG signals of the subjects suffering from HD were considered against the healthy subject and processed using Fisher's linear discriminant (FLD) method, likelihood ratio method (LRM), and an MLP-NN with a single hidden layer, the test was able to classify the data best using NN [23]. Alzheimer's disease, on the other hand, is one of the most common causes of memory loss in old age. This disease is genetically transmitted, and the patient suffering from Alzheimer's shows a gradual loss of cognitive and locomotive abilities starting with its onset. There are only a few treatments commercially available that are used for Alzheimer's such as acetylcholinesterase inhibitors and psychotherapy. Owing to the lack of a cure for Alzheimer's, its growing prevalence, and the need for medical help, early diagnosis is one of the important steps toward administering the disease. It has been observed using tests that with the onset of the disease, there is a surge in delta and theta power bands of EEG waveforms.

### ***3.4 CI in the Analysis of Gait and Movement Patterns***

Several ailments of old age and faulty connections between neural and musculoskeletal systems result in improper and often restricted movement, especially for the elderly where gait disorders can cause severe bone damage and might prove to be fatal in case of a fall. The studies have found that the elderly patients required assistance to get back up and the elderly can suffer from dehydration, pneumonia, pulmonary embolism, hypothermia, or rhabdomyolysis (the toxic breakdown of muscle fibers). Similar is true for patients suffering from diseases like cerebral palsy (CP) who need round-the-clock personal assistance and are often find it difficult to access regular health checkups. Earlier, gait analysis was restricted to sports-related activities to monitor athletes and their movements, but with the growth of technology, gait analysis has found applications for a wide-ranging audience. Since our movement and gait are influenced by multiple directly or indirectly related factors that form an underlying basis of gait disorders, balance, and postural disorders and rehabilitation, this is also leading the field of development of the design of artificial limbs for amputees and the development of exoskeletons. The uniqueness of each individual's gait creates an unprecedented amount of data to be

handled and monitored based on complex and interdependent nonlinear correlations between gait parameters which are aided by the development of CI. A blend of mechanisms is capable of making efficient decisions when supplied with atypical data using several techniques like supervised learning, fuzzy logic, and evolutionary optimization methods. This not only helps in the reduction of diagnosis time but also remedies the computing facilities and curtails operation costs.

The CI has found applications in areas as diverse as normal gait research, gait event detection, gait disorder diagnosis, gait disorder prevention, and gait prosthesis. One of the primary techniques used in gait and movement patterns and their research is ANN. These applications are primarily used to diagnose gait abnormalities and to administer treatment and interventions. Neural networks have also been applied to joint kinematics data for identifying normal gait parameters like a normal walking, leg length difference, and leg weight difference using angles at joints, hips, and knees. In this research, transformed Fourier coefficients were used as input, and an accuracy of 83.3% was achieved when performed on a small group of ten individuals. To extrapolate even further, the NNs have been used for identifying pathological gait from normal gait. Earlier it was done using an EMG-based model and then using vertical ground reaction forces recorded on two force plates using NN classifiers. As people grow old, people tend to experience a change in gait patterns as they age. For this purpose, the differences in a person's gait were measured by using joint angles, foot ground reaction forces, and several other gait parameters using standard BP, scaled conjugate gradient, and Bayesian regularization algorithms. All three algorithms provided high accuracy to differentiate and provide classification analysis between gaits of young and old individuals and were able to plot different parameters like specificity, sensitivity, and ROC area based on the inputs. Furthermore, the research was extended to classify parameters to identify risk-prone elderly individuals [24]. This was done with the help of minimum toe clearance (MTC) between the toe and ground during the swing phase of the gait cycle. For inputs in this research, histogram plot of MTC during the swing phase was used which was observed during continuous treadmill walking. The various inputs derived from the histogram were then applied to a three-layer NN model with a BP error correction algorithm. This was helpful to create a relation between MTC and individual categories such as balanced or imbalanced individuals.

Further, fuzzy logic has been used under the CI paradigm to classify individuals with different gait disorders, such as in the research to classify healthy individuals from patients suffering from ankle arthrodesis using features extracted from Euler angles from the kinematics of the foot. Further, with the use of stride length and cadence as inputs and fuzzy clustering techniques, O'Malley et al. were able to classify healthy gait and CP children using a relationship between MTC and gait of healthy people prone to falls and trips which indicated 95% accuracy in classifying balance-impaired and healthy gait patterns [25].

## **4 Emerging Trends in Computational Intelligence-Based Healthcare Sector and Applications**

Along with the existing applications of CI in different spheres, the research and development of CI have paved the way for several new fields. This section discusses different up-and-coming areas where CI is being applied for fresh perspectives.

### ***4.1 Human-Machine Interfaces in IoMT***

Neurological disorders create an enormous burden on clinical systems and public health services since the risk of neurological disorders increases with age, thereby reducing the chances of full recovery in case of motor disability. It is generally observed that in these disorders, disruption occurs at one of the stages causing motor impairment such as an injury to the spinal cord, the signals do not get transmitted from the brain to muscle groups due to loss of effective transmitting medium, while in case of brain damage, there is a loss of motor function, muscle atrophy, and reduced muscle reflexes and limb movement. For motor rehabilitation, it is assumed that the muscular potential remains intact, but the nervous system does not generate an appropriate neural signal or there are “transmitting” errors.

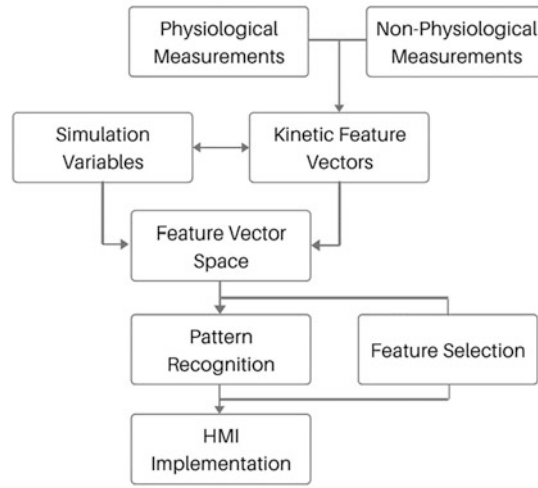
The existing rehabilitation system is created with the help of interdisciplinary groups of professionals who use the remaining neurological and muscular potential to achieve the maximum neuromuscular activity. This is done by reinstating the neuromuscular pathways, retraining the brain functions, and restoring brain and muscular activity. However, even with the advancements done so far, the rehabilitation phase is considered to be highly economically taxing and time-consuming. Therefore, there exists a growing need for the implementation of CI techniques and IoMT for tailoring the rehabilitation methodology for catering to a wide variety of disabilities. Figure 6 presents the optimal model design for an HMI system.

Human-machine interface (HMI) forms an interactive relationship between a person and machine such that real-time inputs from the user can be converted into system commands. They have been used extensively for their user-friendliness and their unique capability to detect minuscule kinematic and kinetic movements and features in the body like joint angles and step length as well as brain activity using EEG and EMG signals. The nonphysiological data is generally recorded using gyroscopes, accelerometers, and force scopes which use IoMT for effective transmission of data from these sensors for processing, while the physiological data is detected and recorded using electroencephalogram and electromyography signals further transmitted for real-time pattern recognition and control signal generation. Processed data delivers signals to the stimulators and exoskeletons providing motor support to the individuals in rehabilitation. In the aforementioned process, it becomes pivotal to convert physiological or nonphysiological data into instructions to the system.



**Fig. 6** Instruction pathway for human-machine interface system

OPTIMAL MODEL DESIGN FOR HMI IMPLEMENTATION



The physiological data has been classified using k-nearest neighbor, SVM with different kernels, and linear discriminant analysis for motor functions. Similarly, the use of fuzzy logic for classification along with ANNs and convolutional NNs has been harnessed for HMI systems [26]. The use of the aforementioned classifiers has greatly reduced computational cost and complexity and increases accuracy, sensitivity, specificity, and realistic operations while maintaining safety standards.

## 4.2 Emotion Classification in Medical Industry

The development of smartphones to cater to the varying needs of the user based on geography, age, gender, occupation, and social activity and has made huge strides. The tailoring of applications and user-friendly choices based on the aforementioned parameters is now being tested in a new paradigm, emotions. Emotions are complex neurophysical states of the mind that are expressed based on external stimuli, physiological state, and human interactions. A field of computer science that deals with the detection and assessment of emotional state is called affective computing. This is done by assessing the human emotional state of the user from the various parameters received and collected from smartphones such as facial expressions, posture, gestures, and typing speed.

To procure parameters that effectively detect and recognize emotions is critical for the development of affective computing in smartphone technology without adding a burden of external sensors to the device. A study proposed the use of physiological signals and consisted of characteristic waveform detection, feature extraction, and emotion classification using support vector machine which allowed

emotion detection for three and four emotions with an accuracy of 78% and 61%, respectively [27]. As discussed earlier, the use of typing speed has also been used to classify human emotion into 15 predetermined states using the C4.5 decision tree classifier [28]. The way of smartphone use has also been used as a determinant for assessing the mood of the user by the use of a smartphone software system called MoodScope [29]. There have been attempts to classify human emotions during video telecommunications with medical staff deriving input from the facial features of the people.

### ***4.3 Emerging IoMT-Based Optimized Wearable Technology***

Much like CI, emerging wearable sensors have found growing relevance in the healthcare industry for tracking vital diagnostic signals on-the-go and, thereby, enabling both the patients and practitioners for the low-cost and pervasive monitoring system by linking different ambient devices. Over the years, the number of wearable infrastructure devices and technology has evolved for a variety of purposes; a few of them include monitoring of physiological data such as ECG, EMG, and EEG, chemical data such as blood sugar level, and optical data such as oximetry; tracking motion, physical activity, and location; and maintenance and management of therapy and treatment purposes such as the delivery of drug packages and chronic pain relief. One of the foremost applications of IoMT has been alerting healthcare professionals in case of a medical emergency with the help of on-body contact sensors and peripheral noncontact sensors.

Wearable technology has been a boon for the patients of elderly suffering from Parkinson's disease, Alzheimer's disease, and dementia along with cognitively challenged patients by helping them to make the right decisions for activities of daily living (ADL) [30]. Not only are they useful for patients, but they have also found equal prominence for monitoring health status and motion and location tracking of healthy individuals through real-time tracking and distinctive feedback system. This has further advanced the research for body-worn smart clothing and other wearable pieces of equipment [31].

The success of wearable technology can be attributed to its miniaturization of hardware sensors, customized design, remote patient-practitioner interaction, personalized medication, and robust management.

### ***4.4 Evaluation and Categorization of Cardiovascular Diseases***

For recognition and detection of CVDs, b-mode ultrasound imaging of the common carotid artery for measuring the thickness of intima-media thickness is performed. Using ultrasound scanning, we can assess the thickness of the innermost layers of the arterial wall and give the distance between lumen-intima and media-adventitia.

Studies suggest that there exists a direct correlation between the thickening of IMT of the common carotid artery and the increasing risk of strokes. The questions arising in the early stages of studies aimed to compare the IMT on the left- and right-hand side of CVD patients and normal healthy individuals, how different ages affect the IMT, and how automated measurements of IMT are better than manual methods. This ultimately aims to classify data procured from studies. Several methods were proposed to measure IMT through segmentation of intima-media complexes such as the semiautomatic method based on snakes and automated segmentation based on active contours with and without edges. All the mentioned methods were applied to normalized rectangular section by application of speckle reduction filtering before segmentation.

The studies have suggested that there exists a significant difference between left and right side IMT in the case of CVD patients. However, the difference was not that pronounced for healthy individuals; however, few studies tend to challenge these findings. Studies even suggest significant differences between healthy individuals and CVD patients' IMT measurements on both sides, where IMT measurements for CVD-affected groups were higher. The studies established a linear relationship between the IMT measurements and age group for both manual and automated segmentation. The classification methods used in this study were the C-SVM network using the Gaussian radial basis function (RBF) kernel and the linear kernel. However, the correct classification score achieved in these methods was in the range of 61–67% [32].

#### ***4.5 Leveraging Social Media Healthcare for Prognostication and Effective Decision-Making***

An exponential spike in the usage and consumption of social media networks (SMNs) has been witnessed in the past decade for fluid data transmission, sharing opinions, ideas, facts, and news and various multimedia files for people to connect globally. This information which is shared every day has proven its significance among the modern world in tracking the trends of positive and negative public healthcare policy opinions are powerful indicators for designing forecasting and prevention mechanisms against disease outbreaks. CI and its applications have grown exponentially and found applications in the field of healthcare coupled with data from social media platforms.

Virus outbreaks of contagious diseases of varying severity have been recurrent and frequent all over the globe, for example, measles and influenza outbreaks in Europe and hay fever outbreaks in Australia. The underlying factor among all these outbreaks is that these diseases are preventable when adequate corrective measures are taken beforehand. Therefore, with the help of CI techniques, which can relate inconsistent, nonlinear data from different sources and other ambient parameters like climatic conditions and seasonal changes to predict the disease outbursts weeks

before the outbreak? For example, the combined use of conventional data sources such as the frequency of hospital visits and data from social media was proposed for influenza prediction [33]. The methodology was found to be highly efficient as it was able to predict the accurate influenza weekly predictions weeks before traditional data sources. Furthermore, in Australia, researchers used text mining and real-time analytics along with changing weather conditions to identify and predict hay fever in Australia based on data collected from Twitter. In research conducted it was found that Twitter saw a rise in the number of positive tweets supporting vaccination during the outbreak in Europe [34]. This, however, was accompanied by a similar spike in the number of negative tweets during 3 months of the outbreak. This data was conclusive since it depicted that the people engaged in vaccination-related debates online and how the opinions regarding vaccination vary across the spectrum of age, gender, and ethnicity.

Generally, it is observed that the emergence of virus illness outbreaks is followed by the resurgence of anti-vaccination movements. These movements disseminate information that challenges “good” and “healthy” public health practices and are proven hurdles of universal protection against diseases. In recent times, anti-vaccination movements have seen a rise post-outbreak where we witness the consumers abstaining and losing faith in vaccines and medical products. This was observed during an illegal Chinese vaccine distribution network where the respondents lost their trust in vaccines and showed reluctance in vaccinating their children while maintaining their trust in the scientific community and medical professionals [35]. Misinformation spreading via social media can be used to peddle negative information against disease resurgence. With vaccine refusal due to lack of trust and misinformation being equally present on social media networks, frameworks have been suggested to make interventions to present evidence-based data while maintaining sanctity between privacy, liberty, and public health practices.

CI techniques to identify mental health issues to identify, diagnose, monitor, and treat patients via social media have been increasingly used with high precision and accuracy. Data collected from Twitter was researched using text specificity for prediction, a model used in CI. The model was able to identify with high accuracy patients suffering from mild/severe cases of depression. Mechanisms have also been applied to track food, dietary habits, and environmental studies based on the data mined from social media networks. In a study conducted in Las Vegas, this method was used to track foodborne illnesses from a venue. The method in real time tracked more than 16,000 tweets from Las Vegas within 5 days and was able to predict eateries, restaurants, and cafes with sub-par food security standards. It was found that the model could predict nearly 9000 cases of foodborne illnesses and prevent nearly 550 hospitalizations each year in the city of Las Vegas. Banyal et al. suggested using the ANN for smog prediction using data mined from social media platforms to prevent road accidents and other disasters [36].

## 5 Conclusion and Future Scope

CI, which witnessed the rise to prominence in the past two decades, is slowly becoming an indispensable resource for the physicians and medical professionals for early detection, diagnosis, classification, and treatment of diseases and disorders by reducing human intervention and for solving several biomedical engineering problems. Although the CI techniques have been accepted in the medical industry with caution, they have been able to reduce the subjective factor of the diagnostic skills of the medical professional. Achieving a significant success rate of accuracy, specificity and sensitivity have been major contributing factors for this growth in the number of CI techniques being accepted in clinical practice and research. The application of CI in CVD, neuromuscular and neurological disorders, and gait and movement impairment as discussed in the early chapters reflects the importance of early detection in healthy individuals, which could result in a huge impact on society and the economy. The use of ECG-, EMG-, and EEG-recorded signals could help in reducing the overall cost of development of expensive equipment, which is virtually not feasible in countries with low economies wherein such diseases have been on the rise and have accounted for high mortality rates.

Along with the growing acceptance of these techniques, there is a multitude of challenges, including the accuracy of the techniques. The accuracy of the technique is highly dependent on the data provided to it in the form of input which is often lacking and highly unreliable and has to be tested multiple times to ensure reliability. With progress in this technology, we have realized that NN, which was earlier popular, is now being replaced by newer techniques such as support vector machines and fuzzy logic [37]. The future trends which have been gaining traction are prediction, rehabilitation monitoring, early warning, and healthcare information system [38]. All these developments would be helpful in making healthcare an all-pervasive, affordable, and efficient future.

## References

1. N. Varuna Shree, T.N.R. Kumar, Identification and classification of brain tumor MRI images with feature extraction using DWT and probabilistic neural network. *Brain Inf.* **5**(1), 23–30 (2018)
2. K.H. Alaa, A.S. Hashim, W.A. Awadh, Clinical data warehouse a review. *Iraqi. J. Comput. Inf.* **44**(2) (2018)
3. M. Rao, B. Eswara, Head, Comparative analysis of pattern recognition methods: An overview. *Indian J. Comput. Sci. Eng.* **2** (2011)
4. M.E. Cohen, D.L. Hudson, L.T. Mann, J. van den Bogaerde, N. Gitlin, Use of pattern-recognition techniques to analyze chromatographic data. *J. Chromatogr. A* **384**, 145–152 (1987)
5. M.B. Sesen, A.E. Nicholson, R. Banares-Alcantara, T. Kadir, M. Brady, Bayesian networks for clinical decision support in lung Cancer care. *PLoS One* **8**(12), e82349 (2013)
6. P. Gupta, A. Pandey, P. Akshita, A. Sharma, Iot based healthcare kit for diabetic foot ulcer. *Lect. Notes Electrical. Eng.*, 15–22 (2019)

7. A.H.-T. Li, S.D. Chao, W-C. Chen, M.-F. Lin, Wearable device system capable of effectively treating onychomycosis. 2018 international automatic control conference (CACs), (2018)
8. C-N. Lee, V.H. Fong, Y-T. Chu, L. Cheng, H-W. Chuang, C-Y. Lo, A wearable device of gait tracking for parkinson's disease patients. 2018 International Conference on Machine Learning and Cybernetics (ICMLC), (2018)
9. F. Rosenblatt, The perceptron: A probabilistic model for information storage and organization in the brain. *Psychol. Rev.* **65**(6), 386–408 (1958)
10. S. Banyal, K. Bhardwaj, D. Sharma, Probabilistic routing protocol with firefly particle swarm optimization for delay tolerant networks enhanced with chaos theory. *Int. J. Innov. Comput. Appl.* **12**(2), 25–37
11. M. Xiao, X. Liu, J. Ji, M. Li, J. Li, Y. Lin, W. Sun, et al., Multiple approaches for massively parallel sequencing of SARS-Cov-2 genomes directly from clinical samples. *Genome Med.* **12**(1) (2020)
12. K. Bhardwaj, S. Banyal, D. Sharma, Artificial intelligence based diagnostics, therapeutics and applications in biomedical engineering and bioinformatics. *Internet Things Biomed. Eng.*, 161–187 (2019)
13. A. Esteva, B. Kuprel, R.A. Novoa, J. Ko, S.M. Swetter, H.M. Blau, S. Thrun, Dermatologist-level classification of skin Cancer with deep neural networks. *Nature* **542**(7639), 115–118 (2017)
14. M. Ward-Peterson, J.M. Acuña, M.K. Alkhalifah, A.M. Nasiri, E.S. Al-Akeel, T.M. Alkhalidi, S.A. Dawari, S.A. Aldaham, Association between race/ethnicity and survival of melanoma patients in the United States over 3 decades. *Medicine* **95**(17), e3315 (2016)
15. M.T. Banday, N.A. Shah, A concise study of web filtering (2010). All Sprouts Content. 352. [https://aisel.aisnet.org/sprouts\\_all/352](https://aisel.aisnet.org/sprouts_all/352)
16. R. Andreao, B. Dorizzi, J. Boudy, ECG signal analysis through hidden Markov models. *IEEE Trans. Biomed. Eng.* **53**(8), 1541–1549 (2006)
17. E.Z. Ferdousy, M.M. Islam, M.A. Matin, Combination of naive bayes classifier and K-nearest neighbor (cNK) in the classification based predictive models. *Comput. Inf. Sci.* **6**(3), 48 (2013)
18. S. Osowski, L.T. Hoai, T. Markiewicz, Support vector machine-based expert system for reliable heartbeat recognition. *IEEE Trans. Biomed. Eng.* **51**(4), 582–589 (2004)
19. S. More, J. Singla, S. Verma, U. Ghosh, J.J. Rodrigues, A.S. Hosen, I.H. Ra, Security assured CNN-based model for reconstruction of medical images on the internet of healthcare things. *IEEE Access* **8**, 126333–126346 (2020)
20. H. Xie, H. Huang, Z. Wang, A hybrid neuro-fuzzy system for neuromuscular disorders diagnosis, in *IEEE international workshop on biomedical circuits and systems*, (IEEE, 2004), pp. S2–S5
21. C.C. Pang, A.R. Upton, G. Shine, M.V. Kamath, A comparison of algorithms for detection of spikes in the electroencephalogram. *IEEE Trans. Biomed. Eng.* **50**(4), 521–526 (2003)
22. R. Harikumar, B.S. Narayanan, Fuzzy techniques for classification of epilepsy risk level from EEG signals, in *TENCON 2003. Conference on convergent Technologies for Asia-Pacific Region*, vol. 1, (IEEE, 2003, October), pp. 209–213
23. M. De Tommaso, F. De Carlo, O. Difruscolo, R. Massafra, V. Scirucchio, R. Bellotti, Detection of subclinical brain electrical activity changes in Huntington's disease using artificial neural networks. *Clin. Neurophysiol.* **114**(7), 1237–1245 (2003)
24. W.L. Wu, F.C. Su, Potential of the back propagation neural network in the assessment of gait patterns in ankle arthrodesis. *Clin. Biomech.* **15**(2), 143–145 (2000)
25. R. Begg, R. Hassan, S. Taylor, M. Palaniswami, Artificial neural network models in the diagnosis of balance impairments, in *Proceedings of 2005 international conference on intelligent sensing and information processing*, (IEEE, 2005), pp. 518–522
26. Y. Zhang, Y. Wang, G. Zhou, J. Jin, B. Wang, X. Wang, A. Cichocki, Multi-kernel extreme learning machine for EEG classification in brain-computer interfaces. *Expert Syst. Appl.* **96**, 302–310 (2018)
27. K.H. Kim, S.W. Bang, S.R. Kim, Emotion recognition system using short-term monitoring of physiological signals. *Med. Biol. Eng. Comput.* **42**(3), 419–427 (2004)

28. C. Epp, M. Lippold, R.L. Mandryk, Identifying emotional states using keystroke dynamics, in *Proceedings of the sigchi conference on human factors in computing systems*, (2011), pp. 715–724
29. R. LiKamWa, Y. Liu, N.D. Lane, L. Zhong, Moodscope: Building a mood sensor from smartphone usage patterns. in, *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, (2013, June), pp. 389–402
30. Q. Zhang, L. Ren, W. Shi, HONEY: A multimodality fall detection and telecare system. *Telemed. e-Health* **19**(5), 415–429 (2013)
31. K. Mankodiya, Y.A. Hassan, S. Vogt, H. Gehring, U.G. Hofmann, Wearable ECG module for long-term recordings using a smartphone processor, in *Proceedings of the 5th international workshop on ubiquitous health and wellness, Copenhagen, Denmark*, vol. 2629, (2010, September)
32. C.P. Loizou, A. Nicolaides, E. Kyriacou, N. Georghiou, M. Griffin, C.S. Pattichis, A comparison of ultrasound intima-media thickness measurements of the left and right common carotid artery. *IEEE J. Transl. Eng. Health Med.* **3**, 1–10 (2015)
33. M. Santillana, A.T. Nguyen, M. Dredze, M.J. Paul, E.O. Nsoesie, J.S. Brownstein, Combining search, social media, and traditional data sources to improve influenza surveillance. *PLoS Comput. Biol.* **11**(10), e1004513 (2015)
34. M. Dredze, D.A. Broniatowski, M.C. Smith, K.M. Hilyard, Understanding vaccine refusal: Why we need social media now. *Am. J. Prev. Med.* **50**(4), 550–552 (2016)
35. Z. Gu, P. Badger, J. Su, E. Zhang, X. Li, L. Zhang, A vaccine crisis in the era of social media. *Natl. Sci. Rev.* **5**(1), 8–10 (2018)
36. S. Banyal, K.K. Bharadwaj, D.K. Sharma, A. Khanna, J.J. Rodrigues, HiLSeR: Hierarchical learning-based sectionalised routing paradigm for pervasive communication and resource efficiency in opportunistic IoT network. *Sustainable computing: Informatics and systems*, (2021), p. 100508
37. P. Singh, A. Nayyar, A. Kaur, U. Ghosh, Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet* **12**(4), 61 (2020). <https://doi.org/10.3390/fi12040061>
38. A.S. Hosen, S. Singh, P.K. Sharma, U. Ghosh, J. Wang, I.H. Ra, G.H. Cho, Blockchain-based transaction validation protocol for a secure distributed IoT network. *IEEE Access* **8**, 117266–117277 (2020)

# A Review on Security and Privacy of Internet of Medical Things



Mohan Krishna Kagita, Navod Thilakarathne, Thippa Reddy Gadekallu, and Praveen Kumar Reddy Maddikunta

## 1 Introduction

A network of medical devices and people are envisioned by the Internet of Medical Devices (IoMT) by which the data of healthcare are exchanged with the help of wireless communication [1]. Since the advanced technology and the population are increasing and growing all over the globe day by day, the services of the healthcare sector and the cost of healthcare are also increasing every day [2]. In the coming days, if the healthcare sector and the Internet of Medical Things work together, then the quality of life can be improved, much better care services will be offered to the population, and more systems can be created that will be cost-effective too [3].

The lives are changing in such a way that was never imagined by anyone in the past with the help of IoT and IoMT [4]. Not like the regular paradigm, each object is connected in the world of the Internet of Things, and every object is considered as the smart object. “Internet of Things” is a network of things that are physical and virtual, and which is dynamic and self-configuring as well. Communication protocols that are interoperable, media, and standards are the power backups of the Internet of Things. “Internet of Things” is said to be the latest version of technologies such as information and communication [5]. The Internet of Things is having the identities and attributes that can connect the network of information

---

M. K. Kagita

School of Computing and Mathematics, Charles Sturt University, Melbourne, Australia

N. Thilakarathne

Department of ICT, University of Colombo, Colombo, Sri Lanka

e-mail: [navod.neranjana@ict.cmb.ac.lk](mailto:navod.neranjana@ict.cmb.ac.lk)

T. R. Gadekallu (✉) · P. K. R. Maddikunta

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

e-mail: [thippareddy.g@vit.ac.in](mailto:thippareddy.g@vit.ac.in); [praveenkumarreddy@vit.ac.in](mailto:praveenkumarreddy@vit.ac.in)



like the Internet, and able to work as sensors, data processors, networking, and communication tools. New challenges are opened in the domain of the healthcare sector by the Internet of Things (IoT), in terms of appliances that are smart, which is known as the Internet of Medical Things. Significant advantages are offered by the Internet of Medical Things for the people's well-being by improving the quality of their life and dropping down their medical expenses.

Since the number of patients is increasing every day, the regular and traditional systems of the healthcare sector are suffering so many challenges. The Internet of Medical Things is introduced so that the issues and challenges can be addressed; the accuracy, reliability, and efficiency can be increased by equivalent time; and the effectiveness of the domain of the healthcare sector can also be increased. To give a much more effective and efficient response to the needs of the patients, Internet of Medical Things is considered as the process of enhancement and investment as well [6]. There are various issues and challenges that are faced by IoMT like no proper security system, problems in privacy measures, no proper training, and awareness regarding IoMT. Several applications of the Internet of Medical Things that are very closely associated with the sensitive services which are related to the healthcare sector are handling the information of the patients which are very private and sensitive such as the name of the patient, their address, and their conditions related to health [7]. To preserve the privacy of the patient without going down the level of security is the most challenging part of the domain of IoMT. It is very important to have a solution for security and privacy in IoMT which includes very little computation involvement and which requires very few resources [3].

In the smart ecosystem of healthcare, the major step is the utilization of the potential of the technologies that already exist, to deliver the services that are best for the users and improve their life in a much better way. Wireless sensors are very critical elements. They are used to monitor the health status of the patients remotely and then communicate the information to the caregivers by the help of information and communication technologies [8]. The Internet of Medical Things acquires significant help from an empowering technology like artificial intelligence which is assisting the experts of the medical field in their proficiency areas like their clinical decisions [9, 10]. By the use of the data which is generated by the professionals of the healthcare feedback the feed backs of the patients, the computers are learning the normal and abnormal decisions with the help of techniques such as machine learning and deep learning.

There is so much use of sensors of body sensors in the medical field to get the data of the patient easily from distant places instead of connecting with several biosensors and utilizing lots of money. Due to the issues of hacking, there is a threat of security while accessing the body sensor network; therefore, the sensitive details of the patients are secured by developing a secured fuzzy extractor and combining it with a fuzzy vault to provide more security by the use of biometric key authentication system [11].

Since there is a huge development in the communication system in recent years, there is wide use of the Internet of Medical Things in the healthcare sector. With the help of IoMT, the health data of the patient can be continuously monitored without

the involvement of the laboratories by the use of wireless healthcare techniques, and it will also improve the quality of life all over the world [10]. Body sensor network helps to monitor the health data of the elderly people and the children as well by their well-wishers in a much effective manner since they are considered as the major population of the globe and are the main concern by their well-wishers in terms of their health issues. IoMT is dependent on the healthcare systems that are using physical information like body temperature, skin resistance, signals of ECG, and EEG which is taken as the inputs by the sensor network known as body sensor network or BSN [12].

## 2 Risks of Internet of Medical Things

There are so many risks that are associated with the deployment of IoT of medical in the domain of healthcare. Some of them are:

1. The medical condition of the patient and the reputation of the hospital can be seriously affected if the personal information of the patient is disclosed.
2. The medical complication will be generated if the transmitted data is altered and modified by any medical device due to the falsification of data which will lead to the incorrect medical description and high drug dose [13].
3. Sometimes the employees that are unsatisfied with their job or when they are associated with some organized crime activity or being bribed leak the medical details and the crucial information of the patients which leads to the risk of privacy and life of the patient.
4. Due to lack of training, the nurses and doctors can bring in permanent disabilities or even sometimes losing the life of the patient.
5. The life of the patient can be seriously affected, and sometimes they are led to disabilities and fatalities due to the inaccurate medical operations done by some specialized robots [14].

Despite all these challenges and risks, it is seen that the Internet of Medical Things is the combination of reliability and safety of the devices that are used in the medical field that are traditionally used and the dynamic, scalable, and generous capability of traditional IoT. A combination of “Internet of Medical Things” and “Internet of Things” is solving issues of the elderly and the diseases that are chronic by managing so many devices that are deployed for many patients, and at the same time, they are enough generic to look after so many diseases which require hydrogenous monitoring and actuation. Standardization is the major challenge that is faced by the Internet of Medical Things. It is very important to have the standardization of all the medical devices that are working together, and the vendors need to go for the correct security measures to have the protection of getting hacked [15]. The Internet of Medical Things is also providing the solutions to the challenges like the mobility of the patient which means that if the patient is unable to move, even then he can be monitored, and medical facilities can be provided at their

comfort zone by the use of IoMT. Instead of having so many issues, risks, and challenges, there is a demand for the latest technological issues for the systems of healthcare; developers are trying to give the solutions to these visitors to change the way of delivering better healthcare to the world.

Since the use and development of medical devices that are connected and distributed, the advent of IoT of medical is caused, and this also brings in the applications that are promising and potential but are challenging at the same time [16]. There is so much use of a network of body sensors on the Internet of Medical Things to get the data of the patient easily from distant places instead of connecting with several biosensors and utilizing lots of money. The integration of devices that are wearable to the IoMT is more focused instead of medical devices that are personal since they are often coming as wearable devices. Sensors, wearable devices, medical devices, and clinical devices are all connected to form an ecosystem of the Internet of Medical Things. There are some concerns which need to be addressed by the biomedical devices because of the strict ethical standards of the medical community. These concerns are:

1. **Reliability:** Each time the functional goals need to be achieved by a reliable system, which means that in normal operating circumstances, unexpected failure should not accrue. It is mandatory to be reliable for the potential diagnostic nature of systems of IoT of medical so that it can give guaranteed information that is collected.
2. **Safety:** The operating system should not be harmed in any way by a safe system. In terms of the Internet of Medical Things, particularly for the medical actuators, it should have the proven facts that the users will not be harmed by the system in any case.
3. **Security:** The system related to the medical field should all must have protection from the threats and attacks from the external devices since they are collecting very sensitive and personal information of the users [17].

### 3 Literature Review

**Al-Turjman, Nawaz, and Ulusar** (2019) studied the status of the Internet of Medical Things for the industry of healthcare; they had also studied the research and plans of development and their applications [18]. Instead of having so many technical and design issues and challenges, there is an exponential increase in the implementation of the Internet of Medical Things in the healthcare sector. Challenges are depicted, and the generic framework of the “Internet of Medical Things” is shown which is composed of three major components to demonstrate the major challenges like the acquisition of data, gateways for communication, and the servers or the cloud [19]. Sensory technologies and wearable and non-wearable sensors are used to collect the data. To monitor a patient, it is good to use the wearable sensors since it will not interrupt the day-to-day activities of the patients.

It is found that these technologies are helping caregivers and also dropping the cost of healthcare. A long and short range of a communication network for the Internet of Medical Things in different cases is surveyed. It is found that WANs are the very reliable, trustworthy, and robust infrastructure of networks in the industry of healthcare when it comes to the accuracy of the data, mobility, and the safety of the patients, but it is seen that they are consuming so much of power [20]. It is also found that the decision tools are a very good tool to make clinical decisions and enhance the services related to healthcare as it is effective in terms of cost and efficiency as well. Since there is no whole sole model of DM which can perform consistently for all the sets of data, therefore it is advised to the hybrids and combination of various tools that can support all the systems.

**Joyia et al.** (2017) found that there are so many people who had contributed to the Internet of Medical Things in the domain of healthcare and there are so many applications and challenges of IoMT as well when it comes to the services related to the medical and healthcare sector [21]. It is seen that the Internet of Medical Things has so much potential in the medical domain and the work will help the researchers the ones who are working in this field to identify the challenges on the Internet of Medical Things. The researchers will get to know about the applications of IoMT and its use in the healthcare sector.

**Kumar and Parthasarathy** (2020) studied the body sensor network which has the scheme of secure authentication and is effective as well [22]. The algorithm which is proposed by the researchers can solve the problems of damage of data, consumption of more energy, and the delay in the network in a much effective manner [23]. Discrete wavelet transforms are used to extract the features in the signals [24]. Users can decide the level of the filters in the algorithm, and the feature extraction accuracy is increased when the level of filters is increased. The noise ratio of the signal is responsible for the efficiency of feature classification which can be removed by using the technique of effective adaptive filtering [25]. It is found that the noise is reduced to up to 4% by this filter in comparison with other techniques that are used previously that is why it is used to lower down the noise in input signals which are complex as a much effective tool. The techniques which are proposed in the study show true positive with an average of 40% and a false positive rate which is also reduced in comparison with the Bayesian network which was already in use. The total energy consumption is also reduced by up to 20% [26, 27]. The authentication phase and the key generation of the system are aimed at this method. A physical layer needs to be developed in the time ahead, and a more effective communication protocol will be required for the improvement of security in MAC, and besides, to achieve the enhanced overhead efficiency an effective routing protocol will be required to be designed in the time ahead.

**Yaacoub et al.** (2019) concluded that there is a requirement of the design of intrusion detection or a prevention system which is more efficient, and which can cooperate with the honey spots having a dynamic shadow [28]. A security solution is proposed which has five layers for the detection and from the prevention of attacks, and it should have the ability to reduce and correct the damage which is the result of these attacks and preserve the privacy of the patients at the same time [29]. But it

is said that the major challenges which are still surrounding the Internet of Medical Things are zero-day attacks and exploits.

**Alsubaei et al.** (2019) found an Internet of Medical Things Security Assessment Framework which is a web-based application and is dependent on the novel ontological environment, and it ensures the security of the solutions on the Internet of Medical Things [30]. In detail, a list of attributes of assessment is recommended by the Internet of Medical Things Security Assessment Framework in which all the essential security measures are covered. This allows the adopters of the Internet of Medical Things to select and force the security in solutions of the Internet of Medical Things which is based on their security aims and which can be altered in a different scenario. The novelty of the Internet of Medical Things Security Assessment Framework is in their ability to adopt the latest technologies that are emerging and the new stakeholders, granularity, and standard compliance [31]. There are cases where the administrators of the system are all alone responsible for making the decisions that are related to the security, but an excellent opportunity is provided to the stakeholders by this work who had personal experience in the cutthroat sector of security on the Internet of Medical Things. Stakeholders are allowed to get to know about the associated risks which are there with the medical devices, and they can follow best practices to overcome the risks and go for better decisions.

**Cecil et al.** (2018) studied that in the framework of cyber training, there is a very limited scope of surgery training [32]. The professional is trained to do the surgical process in orthopedics only for plastic surgery which is majorly done for the fracture of the femur bone. GENI-dependent networking technologies are playing a great role and support the activities of cyber training [33]. The design of the simulation environment is discussed in detail [34]. In a medical university, the residents of the orthopedic field are using the framework which is based on Internet of Medical Things for their training activities; in their assessment part of studies, they are adopting the frameworks which are based on Internet of Medical Things (IoMT) in their surgical training and education.

**Elhoseny et al.** (2019) studied a group of experimentation which is done by the use of data which is collected from women who are having a high risk of ovarian cancer due to the family history or history of cancer for an individual [35, 36]. While comparing the data with the recurrent neural networks which are also known as RSS with the feed-forward neural network (FFNN) and with some others, it is seen that the method which is proposed is attaining Amax accuracy of the sensitivity of 96.27 and 85.2 of the rates of specificity [27]. The results of the experiments show that the model which is proposed is very useful in detecting cancer at their initial stages. The model can detect the cancer with high accuracy, root means square with low error, sensitivity, and specificity as well.

**Farahat et al.** (2018) studied a model that has real-time security, and it also has an encryption method which is encoded with the authentication [36]. This model can solve the security problems of Internet of Medical Smart Things (IoMST). The Internet of Medical Smart Things is facing a very big issue of real-time security and privacy as well [37]. A technique of run-length encoding is presented in the study

which is followed by the encryption that has a key that is rotating in the system of the patient, and the data is decrepitude which has a rotated key, and it is decoded with the decoding run-length technique in the system of the physician. The integrity of the record is ensured by the digital signature of the patient. Further, the study can be done by focusing on developing a shield of e-health which will collect all the data from the sensors of the Internet of Medical Smart Things, and a system is developed by them who can do the encryption by using the asynchronous method. If the number of sensors is increased in our system, it can be implemented for solving the problems of big data. Then it is possible to implement a personal blockchain of the health record of the patient [38].

**Gatouillat et al.** (2018) revealed that the validation and verification of the system can also be done along with the robustness, security, and reliability of the system by an approach of cyber-physical systems (CPS) [39]. While designing a biomedical system, this is the crucial question: are cyber-physical systems the much better process of designing for implementing, designing, and deploying such kind of systems in the biomedical field?

**Guan et al.** (2019) found that the technique of machine learning can be used for data processing which is involved in the Internet of Medical Things for the analysis of the medical data and diagnosis of the diseases [40]. At the same time, it is very important to pay great attention to the personal privacy information disclosure so that the personal and sensitive medical data of the patient and the hospital is not leaked out. The technique of cluster analysis plays an important role in a diagnosis of diseases and medical analysis. Efficient Differentially Private Data Clustering Scheme (EDPDCS) which is based on the map-reduce framework is proposed in this study to allow the privacy-preserving cluster analysis on the Internet of Medical Things. It is found that when the data sets of the algorithm of normalized intra-cluster variance are compared with other data set of the algorithms, it is seen that the accuracy of the deferentially private k-means is improved by Efficient Differentially Private Data Clustering Scheme (EDPDCS).

**Dimitrov** (2016) found that the new category of advisors of digital health will emerge in the future. This category of advisors of digital healthcare is skilled, and they are capable of interpreting the data of the health and well-being of the patient [12]. They are helping their clients to avoid their illness which is chronic in nature chronic and their diet-related problems, cognitive function are improved, in achieving mental health, which is improved, and they are also helping their clients in achieving an overall improved lifestyle. Such roles of the Internet of Medical Things are becoming very important due to the elderly of the world population.

**Jin et al.** (2019) found that the prediction of the quantity of the patients from the outside is not a problem of simple time series and there are so many factors of different variety which are nonlinear, and they are influencing this problem [41]. At the same time in some other experiments, a prediction model was proposed which is multidimensional and has a feature of air quality which is much better than other models. Through the analysis of the data of the experiments, it is found that a very important and significant role is played by the indicators of air quality in the prediction of the respiratory clinic of the patients from outside and their visit to

the clinic. The prediction of respiratory consultations and their significant lag effect and a lag prediction of 4 days which has a better effect are discussed in the paper. On the analysis of the results, it is seen that there is a lagging effect of air in respiratory diseases.

**Liu et al.** (2019) studied the involvement of IoT of medical in the lung cancer treatment and the potential application of models of deep reinforcement learning in the diagnosis which involves the computers [42]. Models of deep reinforcement learning are presented in particular which had promised to be used in the localization and treatment of lung cancer. If the tumor of the lung is detected and diagnosed at their initial stages, then the effect of the treatment is improved, and there is a chance of prolonging survival in a much significant manner. The open challenging matters and applications of the model of deep reinforcement learning for the diagnosis and treatment of lung cancer are discussed further in this study. It is seen that there are two major research directs that can be possibly proposed in the future which involves the localization of the tumors and the making of the plan of treating it.

**Wang et al.** (2020) studied and designed an encoder-decoder structure that is densely connected. This structure shares the codes and at the same time integrates the decoders the depths which are different from each other [43]. The structure which is densely connected is correlated by the output of the multiple decoders [44]. An adaptive segmentation algorithm was proposed by the use of this structure for shallow and deep features. The advantages and benefits of the model which is proposed for the complex boundary segmentation were verified when the two sets of data were compared in the horizontal and vertical manner. The analysis of the experiments demonstrates that the algorithm of the depth feature of adaptive segmentation uses the information of different depths and the results of the segmentation which were generated by the decoders of different depth in an effective manner and the final results can be analyzed, and by this the accuracy of image segmentation is also improved.

**Wasankar, Gulhane, and Gautam** (2017) studied the system which is known as K-healthcare which uses four layers to work more closely and because of which the storing and processing is done much efficiently, and along with that the valuable data is retrieved [45]. So many services are provided by this remotely like to prevent and diagnose the disease, assessment of risk, patient health can be monitored, users can be educated and treated by this system. The work which is going on K-healthcare focuses more on the development and deployment in real means [46]. The software can be designed, or an application of the smartphone can be developed in which the data can be directly obtained from the sensors and processed automatically.

**Rubi and Gondim** (2019) found a platform that prepares the data for OLAP application automatically with the help of automatic recording; thus, the privacy of the patient is granted [47]. The application of data mining is simplified by the file system, the techniques of knowledge extraction, and the machine learning training of preprocessed automatic recording which has resulted from the application of a repository of healthcare [48]. A framework of development was implemented for the devices of “Internet of Medical Things,” gateway and the server for fog so that the new sensors of the platform can be integrated, an extension of functionalities



of AE in the gateway and for the new binding protocols that can be implemented. Instead of isolated devices, the healthcare system is enabled which focuses on the data interchange.

**Islam et al.** (2015) surveyed the healthcare technologies that are based on the “Internet of Things” and their diverse aspects and presented the different architectures of healthcare network along with the platforms which support the backbone of “Internet of Things” and facilitate the transmission and reception of medical data [49]. There are so many researches and development efforts that are done in the healthcare services and the applications that are driven by the “Internet of Things” [50]. The details of research activities that are concerned about the Internet of Things and its address to the pediatric and elderly care, supervision of chronic diseases, personal health, and fitness management are provided in the paper. There are so many works going on to advance the sensors, healthcare devices, applications of the Internet, and other various technologies which will motivate the gadgets of healthcare that are affordable and expand the potential of the services that are based on the Internet of Things in the healthcare sector for their development in the future [51].

**Bhat et al.** (2017) address the necessity of the technology of “Internet of Things” with the solutions of e-health and the devices that are wearable so the healthcare of the patients can be improved and, for this, the access to EMR of the patient is provided which is quick and secure [52]. It is seen that the automation of building blocks of “Internet of Things” and the communication of machine to the machine are continued as before, but the layers of the services are added to complete the infrastructure [53]. A smarter approach for health-related services is not provided by the e-health system that is based on the “Internet of Things,” but the process of decision-making becomes more intelligent [54, 55]. In all the aspects, different issues of health are addressed by this system as a mass. As the model of e-health that is proposed has its foundation that is based on the digital world, the outputs are transformed to the second screen and the mobile devices in many easy ways [56].

**Polu** (2019) studied that the checking of the patient from the remote area is incredibly helping the patients and the healthcare experts as well, but at the same time the accessibility of the RPM is yet not possible for the impacted individuals who can rely on the area they belong to and their abilities of remote access [57]. In addition, it is important for the experts to make much more effort with targeted goals to attract the patients and bring them in and spur them for utilizing RPM. At last, the precision of the gadget that is not proved yet is the fundamental disadvantage of this innovation. It is not known for how much time the imprecision will exist; the RPM will remain dubious for so many. The fundamental idea behind the framework that is proposed is to provide the statistics of health to the administrators of well-being and the patients which are accurate and efficient after the execution of an organized cloud of data so that the information can be used by the experts and the patients and determine quick and effective action [58]. The final model which can be used by the doctors for the examination of the patients from anywhere on the globe at any time will be well equipped and loaded with all the features. In case of emergency, an emergency signal or a message will be sent to the doctors by this model along with



the current status of the patient and medical information. For the easier and quicker access to this model from anywhere on the globe at any time, it can be deployed as a mobile app.

## **4 Challenges for Internet of Medical Things**

Standardization is the major challenge that is faced by IoMT. It is very important to have the standardization of all the medical devices that are working together, and the vendors need to go for the correct security measures to have the protection of getting hacked [59]. If all the devices are standardized, then they will be able to provide much more protected, efficient, scalable, consistent, and effective data. There are so many related but not limited challenges to the different constraints of the security of IoT of Medical Things. The novel ontological scenario-based approaches are the present challenges of proposed systems. Fiscal and policy issues are most common challenges in the Internet of Medical Things. Low quality of data acquisition and high-power consumption, data privacy, and CPU capacity security challenges and security threats, and unproved precision of Internet of Medical Things and medical image segmentation are the main challenges of the present proposed systems [60].

## **5 Proposed Solutions for the Current Approach**

Apart from all the success and advantages of proposed Internet of Medical Things, technology is solving the present issues, but with security and privacy concerns, there exist challenge aspects as well [60]. The main challenging issue includes the security issues as the main background to develop the approach based on cloud-connecting database. To overcome the security challenge, we have come up with a new approach that creates a dynamic, connected scheme to merge the advanced digital facilities allowing the medical services. Moreover, further research should collaborate in creating a digital resolution like hybrid approach, telemedical approach, and CPS approach; machine learning (ML), using BP neural acquisitions, fuzzy extractor combined with fuzzy vault approach, and adaptive fully dense (AFD) can be used [61].

## **6 Conclusion**

The Internet of Medical Things is also known as healthcare IoT of medical which involves medical devices and their application that are connected to the systems of healthcare of information technology with the help of the digital world. These devices and the systems are Internet dependent which facilitates the communication

No.	Year/author	IoT medical subverticals	Technologies used	Benefits of the proposed system	Challenges in current approach	Solution for current issues	Drivers of IoT medical	Application
1	Alsubaei et al. (2019)	Security & privacy	Web-based "Internet of Medical Thing" Security Assessment Framework (IoMT SAF)	Security of stakeholders Decision-making process	Security & privacy of the "Internet of Medical Thing" Novel ontological scenario-based approach	Security features in "Internet of Medical Thing" Protection & deference in "Internet of Medical Thing"	Adapt new stakeholders & conformance to technology & medical standards	Healthcare
2	Al-Turjman et al. (2019)	Patient monitoring, sharing information	Sensory technologies, wearable & non-wearable sensors	Workload is decreased Decreased healthcare cost	High-power consumption	A hybrid approach	Additional information is provided in healthcare information systems	Healthcare
3	Banka et al. (2018)	Smart health monitoring	Raspberry Pi	Recording of heart rate, BP of patients			Analyze & predict chronic disorders in the preliminary stage by the use of data mining techniques	Healthcare
4	Bhat et al. (2017)	Removes the physical limitations	Bluetooth Wi-Fi GUIs	Quick & secure access to patients' EMR		Smart approach	Transform the outputs to second screen & mobile devices	Healthcare
5	Cecil et al. (2018)	Orthopedic surgery	GENI-based network	Surgical services by robots	Telemedicine approaches			Healthcare
6	Elhoseny et al. (2018)	Detection of ovarian cancer	SOM ORNN	Early-stage detection of cancers with high accuracy, sensitivity			Classifies ovarian cancer data	Healthcare
7	Farahat et al. (2018)	Real-time security & privacy	Run-length encoding technique	Solve the problem of the security of IOMST	Security privacy standard regulation	Security privacy standard regulation	Records the private blockchain of the patient's healthcare	Healthcare

(continued)

No.	Year/author	IoT medical subverticals	Technologies used	Benefits of the proposed system	Challenges in current approach	Solution for current issues	Drivers of IoT medical	Application
8	Garouillat et al. (2018)	Verification & validation	CPS	Designing, implementing, testing, & deploying The accurate differentially private k-means algorithm		CPS approach	Better control of system Robustness Security Reliability	Healthcare
9	Guan et al. (2018)	Accuracy & efficiency	Cluster analysis			A machine learning approach	Accuracy & efficiency of clustering algorithm	Healthcare
10	Dimitrov (2016)	On-field mobile/tablet technology	Wearable & mobile apps	Hassle-free record management	Fiscal & policy issues		Remote health monitoring	Healthcare
11	Islam et al. (2015)	Security & privacy	IoT-based healthcare technologies	Pediatric & elderly care, chronic disease supervision, private health, & fitness management			The intelligent collaborative security model	Healthcare
12	Jin et al. (2019)	Analysis & prediction	Intelligent sensing technology	Analysis & prediction of medical data	Low quality of data acquisition	Use of BP neural network	Outpatient number prediction	Healthcare
13	Joyia et al. (2017)			Make life more convenient	Data privacy CPU capacity security challenges			Healthcare
14	Kumar et al. (2019)	Network security	Body sensor network The effective adaptive filtering technique	Issues like data loss, energy consumption, & delay in the network are solved effectively	Security threat	Fuzzy extractor combined with fuzzy vault approach	Access to patient's data remotely	Healthcare

15	Liu et al. (2019)	Lung cancer detection	Deep reinforcement learning models	Early detection & diagnosis of lung tumor			Lung cancer localization & treatment	Healthcare
16	Polu (2019)	Health monitoring	Wearable sensors	Remote monitoring	Unproved precision of gadgets		To give accurate & efficient health statistics	Healthcare
17	Rubi et al. (2019)	Data analysis	M2M OLAP	Automatically prepares the data			Ensures interoperability, quality of the detection process	Healthcare
18	Wang et al. (2020)	Object detection	Encoder-decoder structure UNet structure	Can extract various features from all layers adaptively	Medical image segmentation	Adaptive fully Dense (AFD) neural network for CT image segmentation	Accurate image segmentation	Healthcare
19	Wasankar et al. (2017)	Prevention & diagnosis	RFID, IPv6, cloud computing	Efficient storing, processing, & retrieving of valuable data		Data is directly obtained from the sensors & processed automatically		Healthcare
20	Yaacoub et al. (2019)	Safeguard & secure		Train medical & IT staff	Privacy of patients, the confidentiality, integrity, & availability of medical services	Robust "Internet of Medical Thing"	Secure & efficient system	Healthcare

between machines and for the storage of data they are linked to the digital platforms [62]. A wide range of clinical uses are involving Internet of Medical Things such as smart watches and bracelets for medical alerts which can detect the falls of the patients and even can call the medical services in case of emergency. The healthcare industry is transformed by the Internet Medical of Thing as it delivers the targeted and personalized medicine and it also seamlessly enables the communication of medical data. To monitor a patient, it is good to use the wearable sensors since it will not interrupt the day-to-day activities of the patient. It is found that the technologies that are involving the Internet of Medical Things are helping the caregivers and also lowering the cost of healthcare.

## References

1. F. Fernandez, G. Pallis, Opportunities and challenges of the internet of things for healthcare. Proceedings of the 4th International Conference on Wireless Mobile Communication and Healthcare – “Transforming healthcare through innovations in mobile and wireless technologies”, (2014)
2. A. Azab, R. Layton, M. Alazab, J. Oliver, Mining malware to detect variants, in *2014 Fifth Cybercrime and Trustworthy Computing Conference*, (IEEE, 2014, November), pp. 44–53
3. N.N. Thilakarathne, Security and privacy issues in iot environment. *Int. J. Eng. Manag. Res.* **10**(1), 26–29 (2020). <https://doi.org/10.31033/ijemr.10.1.5>
4. S.P. RM, P.K.R. Maddikunta, M. Parimala, S. Koppu, T. Reddy, C.L. Chowdhary, M. Alazab, *An Effective Feature Engineering for DNN Using Hybrid PCA-GWO for Intrusion Detection in IoMT Architecture* (Computer Communications, 2020)
5. M. Alazab, R. Layton, R. Broadhurst, B. Bouhours, Malicious spam emails developments and authorship attribution, in *2013 Fourth Cybercrime and Trustworthy Computing Workshop*, (IEEE, 2013, November), pp. 58–68
6. The Internet of Things for Health Care: A Comprehensive Survey. Available at: <https://ieeexplore.ieee.org/document/7113786>. Accessed June 2020
7. A. Kulkarni, S. Sathe, Healthcare applications of the internet of things: A review. *Int. J. Comput. Sci. Inf. Technol.* **5**(5), 6229–6232 (2014)
8. S. Banka, I. Madan, S.S. Saranya, Smart healthcare monitoring using IoT. *Int. J. Appl. Eng. Res.* **13**(15), 11984–11989 (2018)
9. N. Deepa, B. Prabadevi, P.K. Maddikunta, T.R. Gadekallu, T. Baker, M.A. Khan, U. Tariq, An AI based intelligent system for healthcare analysis using ridge Adaline stochastic gradient descent classifier. *J. Supercomput.* (2020)
10. F. Tao, Y. Zuo, L. Da Xu, L. Zhang, IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. *IEEE Trans. Ind. Inf.* **10**(2), 1547–1557 (2014)
11. G.T. Reddy, M.P.K. Reddy, K. Lakshmana, D.S. Rajput, R. Kaluri, Srivastava, G., Hybrid genetic algorithm and a fuzzy logic classifier for heart disease diagnosis. *Evol. Intel.* **13**(2), 185–196 (2020)
12. D.V. Dimitrov, Medical IoT of medical and big data in healthcare. *Healthcare Inf. Res.* **22**(3), 156 (2016)
13. F.R. Vogenberg, J. Santilli, Healthcare trends for 2018. *Am. Health Drug Benefits* **11**(1), 48 (2018)
14. W. Si, G. Srivastava, Y. Zhang, L. Jiang, Green internet of things application of a medical massage robot with system interruption. *IEEE Access* **7**, 127066–127077 (2019)
15. C. Iwendi, Z. Jalil, A.R. Javed, T. Reddy, R. Kaluri, G. Srivastava, O. Jo, KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks. *IEEE Access* **8**, 72650–72660 (2020)

16. G. Srivastava, J. Crichigno, S. Dhar, A light and secure healthcare blockchain for iot medical devices, in *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*, (IEEE, 2019, May), pp. 1–5
17. W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet Things J.* **6** (2018)
18. F. Al-Turjman, M.H. Nawaz, U.D. Ulusar, Intelligence on the internet of medical things era: A systematic review of current and future trends. *Comput. Commun* (2019)
19. Y.I.N. Yuehong, Y. Zeng, X. Chen, Y. Fan, The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **1**, 3–13 (2016)
20. K. Mekki, E. Bajic, F. Chaxel, F. Meyer, A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **5**, 1–7 (2019)
21. G.J. Joyia, R.M. Liaqat, A. Farooq, S. Rehman, Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* **12**(4), 240–247 (2017)
22. M. Rakesh Kumar, V. Parthasarathy, A secure fuzzy extractor based biometric key authentication scheme for body sensor network on internet of medical things. *Comput. Commun* **153** (2020)
23. C. Iwendi, P.K.R. Maddikunta, T.R. Gadekallu, K. Lakshmana, A.K. Bashir, M.J. Piran, *A Metaheuristic Optimization Approach for Energy Efficiency in the IoT Networks* (Practice and Experience, Software, 2020)
24. P.K.R. Maddikunta, T.R. Gadekallu, R. Kaluri, G. Srivastava, R.M. Parizi, M.S. Khan, Green communication in IoT networks using a hybrid optimization algorithm. *Comput. Commun.* (2020)
25. H. Patel, D. Singh Rajput, G. Thippa Reddy, C. Iwendi, A. Kashif Bashir, O. Jo, A review on classification of imbalanced data for wireless sensor networks. *Int. J. Dist. Sensor Networks* **16**(4), 1550147720916404 (2020)
26. P.K.R. Maddikunta, G. Srivastava, T.R. Gadekallu, N. Deepa, P. Boopathy, Predictive model for battery life in IoT networks. *IET Intell. Transp. Syst.* (2020)
27. Reports & data (2020). Available at: <http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=60129548150>
28. J.P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing the internet of medical things systems: Limitations, issues and recommendations. *Futur. Gener. Comput. Syst* **105** (2019)
29. T.R. Gadekallu, N. Khare, S. Bhattacharya, S. Singh, P.K. Reddy Maddikunta, I.H. Ra, M. Alazab, Early detection of diabetic retinopathy using PCA- firefly based deep learning model. *Electronics* **9**(2), 274 (2020)
30. F. Alsubaei, A. Abuhussein, V. Shandilya, S. Shiva, *IoMT- SAF: Internet of Medical Things Security Assessment Framework* (IoT of medical, 2019)
31. M. Masinde, IoT applications that work for the African continent: Innovation or adoption? in *Proceedings of the 2014 12th IEEE International Conference on Industrial Informatics (INDIN)*, (2014, Porto Alegre), pp. 633–638
32. J. Cecil, A. Gupta, M. Pirela-Cruz, P. Ramanathan, An IoMT based cyber training framework for orthopedic surgery using next generation internet technologies. *Inf. Med. Unlocked* **12**, 128–137 (2018)
33. F. Farivar, M.S. Haghghi, A. Jolfaei, M. Alazab, Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber- physical systems and industrial IoT. *IEEE Trans. Ind. Inf.* **16**(4), 2716–2725 (2019)
34. T. Reddy, S.P. RM, M. Parimala, C.L. Chowdhary, S. Hakak, W.Z. Khan, A deep neural networks based model for uninterrupted marine environment monitoring. *Comput. Commun.* **157** (2020)
35. M. Elhoseny, G.-B. Bian, S. Lakshmanaprabu, K. Shankar, A.K. Singh, W. Wu, Effective features to classify ovarian Cancer data in internet of medical things. *Comput. Netw* **157** (2019)

36. I.S. Farahat, A.S. Tolba, M. Elhoseny, W. Eladrosy, A secure real-time internet of medical smart things (IOMST). *Comput. Electrical Eng.* **72**, 455–467 (2018)
37. M.A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, F. Sallabi, Softwarization of internet of things infrastructure for secure and smart healthcare. *arXiv preprint arXiv:1805.11011*, (2018)
38. M. Numan, F. Subhan, W.Z. Khan, S. Hakak, S. Haider, G.T. Reddy, et al., A systematic review on clone node detection in static wireless sensor networks. *IEEE Access* **8**, 65450–65461 (2020)
39. A. Gatouillat, Y. Badr, B. Massot, E. Sejdic, Internet of medical things: A review of recent contributions dealing with cyber-physical Systems in Medicine. *IEEE IoT Med. J.*, 1–1 (2018)
40. Z. Guan, Z. Lv, X. Du, L. Wu, M. Guizani, Achieving data utility-privacy tradeoff in internet of medical things: A machine learning approach. *Futur. Gener. Comput. Syst* **98** (2019)
41. Y. Jin, H. Yu, Y. Zhang, N. Pan, M. Guizani, Predictive analysis in outpatients assisted by the internet of medical things. *Futur. Gener. Comput. Syst.* **98**, 219–226 (2019)
42. Z. Liu, C. Yao, H. Yu, T. Wu, Deep reinforcement learning with its application for lung cancer detection in medical IoT of medical. *Futur. Gener. Comput. Syst* **97** (2019)
43. E.K. Wang, C.-M. Chen, M.M. Hassan, A. Almogren, A deep learning- based medical image segmentation technique on the internet- of-medical-things domain. *Futur. Gener. Comput. Syst.* **108**, 135–144 (2020)
44. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and privacy in the medical internet of things: A review. *Secur. Commun. Networks* **2018** (2018)
45. D.B. Wasankar, V.S. Gulhane, L.K. Gautam, Application of internet of things in the field of medical and smart health care. *Int. J. Innov. Res. Comput. Commun. Eng.* **5**(5), 9251–9257 (2017)
46. C. Maina IoT at the grassroots—Exploring the use of sensors for livestock monitoring. In *Proceedings of the 2017 IST-Africa Week Conference (IST-Africa)*, Windhoek, Namibia, 30 May–2 June 2017, pp. 1–8
47. J.N.S. Rubi, P.R.L. Gondim, IoMT platform for pervasive health- care data aggregation, processing, and sharing based on OneM2M and open EHR. *Sensors*, 2–25 (2019)
48. A. Azab, M. Alazab, M. Aiash, Machine learning based botnet identification traffic, in *2016 IEEE Trustcom/BigDataSE/ISPA*, (IEEE, 2016, August), pp. 1788–1794
49. R.S.M. Islam, D. Kwak, M. Humaun Kabir, M. Hossain, K.-S. Kwak, The internet of things for health care: A comprehensive survey. *IEEE Access* **3**, 678–708 (2015)
50. Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things. *IEEE Internet Things J.* **4**(5), 1250–1258 (2017)
51. P.A. Williams, V. McCauley, Always connected: The security challenges of the healthcare internet of things, in *Internet of Things (WF- IoT), 2016 IEEE 3rd World Forum on*, (IEEE, 2016, December), pp. 30–35
52. M.I. Bhat, S. Ahmad, A. Amin, S. Ashraf, E-health with the internet of things. *Int. J. Comput. Sci. Mob. Comput.* **6**(6), 357–362 (2017)
53. S. Bhattacharya, R. Kaluri, S. Singh, M. Alazab, U. Tariq, A novel PCA- firefly based XGBoost classification model for intrusion detection in networks using GPU. *Electronics* **9**(2), 219 (2020)
54. S.P. RM, S. Bhattacharya, P.K.R. Maddikunta, S.R.K. Somayaji, K. Lakshmana, R. Kaluri, et al., Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. *J. Parallel Dist. Comput.* **142** (2020)
55. T.R. Gadekallu, N. Khare, S. Bhattacharya, S. Singh, P.K.R. Maddikunta, G. Srivastava, Deep neural networks to predict diabetic retinopathy. *J. Ambient Intell. Humaniz. Comput.*, 1–14 (2020)
56. J. Qi, P. Yang, G. Min, O. Amft, F. Dong, L. Xu, Advanced internet of things for personalised healthcare systems: A survey. *Pervasive Mob. Comput.* **41**, 132–149 (2017)
57. S.K. Polu, IoMT based smart health care monitoring system. *IJIRST-Int. J. Innov. Res. Sci. Technol.* **5**(11), 58–64 (2019)
58. K.D. Lind, Implantable devices: Regulatory framework and reform options. *Insight* (2017)

59. A. Sajid, H. Abbas, K. Saleem, Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access* **4**, 1375–1384 (2016)
60. Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things. *IEEE Internet Things J.* **4**(5), 1250–1258 (2017)
61. D. Ponlap, G. Srivastava, A. Jolfaei, R.M. Parizi, Blockchain technology and neural networks for the internet of medical things, in *IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WK- SHPS)*, (IEEE, 2020, July), pp. 508–513
62. I.B. Ida, A. Jemai, A. Loukil, A survey on security of IoT in the context of eHealth and clouds, in *Design & Test Symposium (IDT), 2016 11th International*, (IEEE, 2016, December), pp. 25–30



# An Introduction to Wearable Sensor Technology



Arthur Medeiros, Lucas Leme, and Gautam Srivastava 

## 1 Introduction

Wireless sensor technology isn't recent, it has been around for a while, and because of that, it is already being applied to several areas, from turning lights on and off to the monitoring of volcanic activities [1]. Wireless sensor network (WSN) is a technology that aims to make human life more comfortable, and that includes healthcare. Wireless medical sensor network (WMSN) is the application of exactly that, with the usage of many biosensor devices, vital signs and other important information can be easily monitored [2].

As technology evolves, new frontiers are reachable. When we talk about sensors or, in the case of medical sensors, wearable ones, this means they can offer more comfort and fewer obstructions to the user [3]. Wearable sensors are rapidly becoming lighter, smaller, and more viable each day, creating the possibility of a larger array of applicability, ranging from gait (posture) analysis [3, 4] to glucose measurement on a person's body [5], as seen in Fig. 1.

An important point in the development of medical sensors, for IoT, is the transmission of collected data to a remote server or a cell phone. This can be done by a variety of wireless technologies; the more commonly employed for BANs are Bluetooth and ZigBee.

ZigBee's main appeals are its low cost, low data-rate solutions with long-lasting battery life, and low complexity. It utilizes 16 channels in the 2.4 GHz in the ISM (industrial, scientific, and medical) band, 10 channels in 915 MHz, and 1

---

A. Medeiros · L. Leme

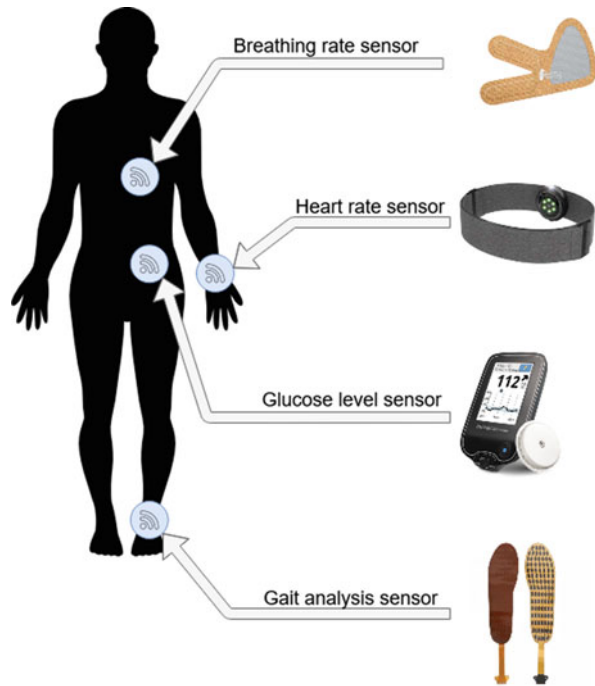
Faculty of Computer Science, Mato Grosso do Sul State University, Dourados, Brazil

G. Srivastava (✉)

Department of Mathematics and Computer Science, Brandon University, Brandon, Canada

e-mail: [srivastavag@brandonu.ca](mailto:srivastavag@brandonu.ca)

**Fig. 1** Examples of wearable sensors available



in 868 MHz. It has a maximum transmission range of 75 m and supports star, tree cluster, and mesh topologies network architectures. ZigBee uses an advanced encryption standard algorithm with 218-bit keys.<sup>1</sup>

Bluetooth is low-power and low-cost RF standard in the 2.4-GHz spectrum. It can frequency hop over 80 channels in the ISM band to avoid interference and fading, also supporting up to 3 Mb/s in enhanced data rate mode. However, encryption is optional using a 64- or 128-bit SAFER+ algorithm, making it vulnerable to attacks and risks [6, 7]. There also exists the BLE (Bluetooth low energy) which uses about 10% less energy than its predecessor making it more desirable for medical sensors.<sup>2</sup>

Lesser-known short-range intra-BAN technologies include infrared data association (IrDA) and the medical implant communication service (MICS). IrDA is a short-range, low-cost, low-power exchange of data over infrared light at speeds up to 1GBs. However, its main drawback is the need for line of sight to communicate, making it less attractive for the Internet of Medical Things (IoMT).

MICS is an ultralow-power, short-range, communication network used worldwide for transmitting data associated with medical implants. It utilizes the 402–405-MHz frequency band, 300-kHz channels, and data transfer rates of 600 kbps. However, MICS shares the same band with other services such as Met Aid and meteorological satellites interfering a possibility. Another problem is the lack of

<sup>1</sup> [www.zigbee.org](http://www.zigbee.org)

<sup>2</sup> <https://www.bluetooth.com/>

**Table 1** Wireless communication comparison

	Frequency	Range	Data Rate
Bluetooth	2.45GHz	1-100m	1-3Mbs
Bluetooth LE	2.45GHz	100m	1-2Mbs
ZigBee	868MHz (US) 915MHz (EU) 2.4GHz	10-20m	20-900kbps
IrDA	Infrared	1m	1Gbs
MICS	402-405MHz	2m	600kbps

a low-power MAC protocol meeting the band requirements for simultaneous data collection from multiple sensors [8].

Table 1 highlights the basic features of the wireless technologies shown above.

Patient data is collected through wearable devices that possess small sensors capable of measuring specific or various physiological parameters, preprocessing hardware, and a communication platform for sending the collected data, be it to a nearby device or a local server [3]. In some cases, the sensors will be worn throughout long periods; if not permanently, this brings into question their wearability.

The sensors must be lightweight, be small, and never hinder a patient’s movement and mobility. Also, because of the need for small sensors, their batteries should be as energy-efficient as possible. However, the battery can be either rechargeable or replaceable; this makes it necessary that they provide long and continuous operation times in between charging or replacement, to ensure that minimal to no data is lost.

The low energy requirement also poses an obstacle to the quality of acquirable data. Recent designs [9] propose the use of flexible, close contact sensors to specific body parts for more varied and precise physiological readings.

Wearable sensors allow the elderly and other people in need of special care to be monitored without the need to be relocated to a hospital or another medical center, creating an opportunity to both a quicker response, by observing fluctuations on vital signs and answering it accordingly, and a more appropriate response, with a deeper knowledge of what the patient is going through.

The means through which the information goes from the wearer to the hands of the specialist is through a series of steps to guide them there. It starts by sending the information gathered by the sensors to a nearby home gateway using a short-range, wireless option, usually Bluetooth or ANT. This information is then sent, through the Internet, to the medical facility responsible for that patient, where it will be analyzed and stored for future reference (Fig. 2) [2]. That does, however, create an opportunity to malicious or miss handle usage of a person’s personal health information, as described in [10]. In [11], the authors present a solution to this problem in the form of blockchain. A blockchain consists of several computers

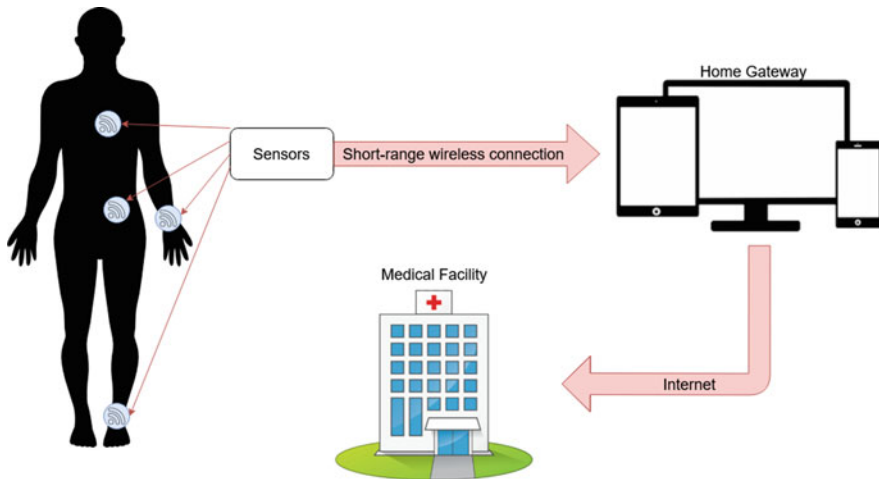


Fig. 2 Path made by the information from the sensors in the body to the medical facility

forming a network of machines that work together to create a distributed data bank and keep the information in it safe and valid.

In this chapter, we will be going over some of the studies that have been done on the area of WMSNs over the past decade and discuss their discoveries, the importance of the work that was done, and what each of them means to the future. We start by taking a look first at the problems, issues, and difficulties that the technology has to deal with before being fully applied and utilized, like the aforementioned security and reliability problem, legal challenges, and application problems.

## 2 Difficulties and Challenges

### 2.1 Security Challenges

In this day and age, being able to keep your private information a secret has gained a considerable amount of importance, and for good reason. In the era of technology, information controls everything that there is to be controlled in our lives, from finances to our social life. Health is no different, keeping a condition or a disease secret, especially if you are a high-profile person, can be of extreme importance, and the leak of this type of information can lead to great displeasure [11].

According to CSO online,<sup>3</sup> cyberattacks toward the healthcare industry will reach over 12 billion dollars in damage by the end of the year 2020; Coveware<sup>4</sup> shows that healthcare is in the top three most targeted industries of last year, behind only professional and software services.

All this information does make the situation look dire, but there is work being done to circumvent it. In 2019, Dwivedi et al. [12] claimed that the use of blockchain technology is the answer to guarantee the security and safety of the information. The system proposed by the author in the paper is blockchain-based, consisting of cloud storage, an overlay network, the healthcare provider, smart contracts, and IoT devices owned by the patient. With a system like this in place, the security of the information is guaranteed, protecting the information from a variety of different types of attacks, like DoS attack, mining attack, storage attack, and dropping attack.

## 2.2 Legal Challenges

Due to the wide range and reach of the IoT, several regulatory agencies have a saying in what can or cannot be developed, used, or sold in the market. In the case of WMSNs, or eHealth in general, new technologies must be accepted and approved. This can vary from country to country, but in the USA, three different agencies need to give the green light, those being the FDA (Food and Drug Administration), the CMS (Centers for Medicare and Medicaid Services), and the FCC (Federal Communications Commission) [13].

The EU in 2016 passed *Regulation (EU) 2016/679 of the European parliament and of the council* [14]<sup>5</sup> laying down rules relating to the protection of natural persons data and rules relating to the free movement of personal data. The regulation other than providing general privacy protection laws that can be applied to any IoT application also mentions the processing of special categories of personal data (article 9) which mentions genetic, biometric, and data concerning health.

In regulation 2016/679 [14], the EU parliament provides obligations and fines in the case of a data breach. In particular, among others, are the obligation of notification, in case of a breach, to the competent regulator and the affected individuals; an increase of fines up to 4% of the global turnover of the previous financial year; and the obligation to implement a privacy and security by design approach.

---

<sup>3</sup> <https://www.csoonline.com/article/3237674/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html>

<sup>4</sup> <https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases>

<sup>5</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>

However, when it comes to eHealth, we must know what can be a medical device or not, for example, a personal smartphone with eHealth applications is not qualified as a medical device [7]. On the other hand, software and cloud platforms have been covered in a green paper issued by the European Commission on mHealth; in this case, it is necessary to verify what its medical purpose is. If the software or cloud-only collects and stores data, it is not considered a medical device. However, if the software is in some way interpreting the data, for instance, a diagnosis or alert message, then it is to be considered a medical device.

### **2.3 Technology Challenges**

One of the biggest difficulties this new technology may face is not the security of its information or the legal repercussions of its application but the usage of such a groundbreaking innovation. The world population is getting older by the year, with improvements in people's lifestyles; we are living better and longer. In some countries in Europe and North America, the elderly population is going to outnumber the young one soon enough. In countries like Germany and Japan, that is already a reality, with a population of elders (65+) outnumbering the young (0–14) by over 10%.<sup>6</sup> This ever-aging population is one of the main groups that could be positively affected by this new technology; the problem is the fact that older people have a resistance to making use of state-of-the-art technology [15]. The people that intend to make use of these new methods of health monitoring will need to be taught how to use them correctly; the involvement of these end users need to be present during the development phase to guarantee the most comfortable and reliable experience.

## **3 The Reach of the Technology**

From wearable shirts that can offer cardiovascular monitoring to invasive enzyme-based glucose sensors, the range of applicability of this technology is seconded only by the impact that it can cause on the lives of its users.

A T-shirt developed by Andreoni et al. [16] is capable of reading heart rate and sending them to a server; the system also comes with a SpO<sub>2</sub> pulse oximeter, a fall sensor, and a smart scale. They achieved this by creating a T-shirt designed with three textile electrodes made from a silver-based conductive yarn integrated into it; they work as electrocardiogram (ECG) electrodes and have the function of recording the Einthoven ECG I-leads. Another advantage of this T-shirt is the absence of conductive paste; these pastes have been known for not being suitable for long-

---

<sup>6</sup> <https://www150.statcan.gc.ca/n1/pub/91-215-x/2018002/sec2-eng.htm>

term usage due to potential toxicity and causing irritation on contact with the skin. Instead of using this paste, the T-shirt makes use of the wearer sweat, moisturizing the sensors and improving the electrical conductivity, and reducing motion artifacts, raising the overall quality of the signal.

One of the most common problems that come with aging is the frequency and damage caused when an elderly person falls. With that in mind, Bertolotti et al. [17] have developed what they call a novel, portable, low-cost nine-degrees-of-freedom measurement unit. This lightweight equipment comes equipped with a three-axial accelerometer, a three-axial gyroscope, and a three-axial magnetometer, to assist motor and balance control abilities by providing a measurement of limb movement. This instrument has been developed as a modular device that can be used in many different ways, including short-term laboratory use, long-term patient/subject's home, or in more complexes, full-body network, for gait analyses or exercise monitoring.

The human body is a biological machine, with a plethora of different parts that come together to create a whole. To be functional this body needs to be balanced and have all components working properly, and to make sure that this is happening, several values are helping us to get a proper read of the situation. One of these values is the pH level of the body; it reveals to us the levels of acidity of our bodies, going from 0 (acid) to 14 (alkali); different body fluids have different values, for example, a healthy stomach has a pH level of around 1.5–2.0; meanwhile, the colon's levels are around 7.9–8.5.<sup>7</sup> According to the ADA (American Dental Association), only 7% of the beverages in the USA have a pH level greater than 4.0 [18], meaning that most of what Americans drink today is extremely acidic, causing the body's pH to drop. An acidic body will cause living cells to die out and tumor cells to be created, considerably increasing the chances for a person to develop cancer. With that in mind, Alam et al. [19] go into detail while reviewing several different types of wireless sensors, including chemical, physical, and electrochemical. They concluded that polymers are a potentially good candidate to be used as material for pH sensors given their chemical stability, flexibility, and low cost.

Diabetes is a major and possibly fatal ailment that affects 422 million people worldwide<sup>8</sup> and, as of now, still has no permanent cure. However, patients can alleviate this disease by utilizing constant blood glucose measurement and insulin intake. There are already sensors in the market for monitoring glucose levels. Nevertheless, with IoT researchers have proposed methods of facilitating the monitoring of this data by doctors and patients. Rasyid et al. [20] propose a system to optimize the sending of glucose estimates using a wireless body area network. The authors utilized a commercial sensor, Arduino Uno, and communication using the Zigbee module. The system stored the received data in a desktop-based application, making it so doctors, nurses, and the patient's relatives could easily access it. Gia et al. [21] propose a real-time IoT-based continuous glucose monitoring system, where

---

<sup>7</sup> <https://www.news-medical.net/health/pH-in-the-Human-Body.aspx>

<sup>8</sup> <https://www.who.int/news-room/fact-sheets/detail/diabetes>

sensor nodes collected several types of data and sent the information wirelessly to a gateway app installed in a smart device making it energy-efficient, which then sent it to a cloud server where medical professionals could access it remotely [22, 23]. The gateway app also had advanced services for the users such as a notification service in case of low glucose levels.

## 4 Future of the Technology

Today this technology faces many challenges when it comes to the implementation and wide usage, from security issues to technological limitations; there are plenty of barriers to surpass and hoops to jump through, but this is changing [24, 25]. With the introduction of new technology like 5G, remote communication is going to be seeing a tremendous impact in its form. The new frontier that 5G brings, not only to the eHealth aspect but to the Internet of Things as a whole, is going to allow for new ideas that were previously impossible to be accomplished to become a reality [26–29].

## 5 Conclusion

The doctor/patient relationship has changed a lot throughout the years, from family doctors that would go to your house and work with only a couple of families to what we see today, with the professional now working from clinics and having the patients go to them, being able to work with hundreds of different clients. With the introduction of remote healthcare and with the use of IoT technology, more specifically IoMT, this relationship can find a middle ground, where neither patient nor doctor needs to be dislocated unless necessary. The usage of wearable sensors helps guarantee the safety and much more comfortable life for those who need constant medical attention, like the elderly or people with compromised health.

## References

1. C. Buratti et al., An overview on wireless sensor networks technology and evolution. *Sensors* **9**(9), 6869–6896 (2009)
2. D. He, S. Chan, S. Tang, A novel and lightweight system to secure wireless medical sensor networks. *IEEE J. Biomed. Health Inform.* **18**(1), 316–326 (2013)
3. S. Majumder, T. Mondal, M.J. Deen, Wearable sensors for remote health monitoring. *Sensors* **17**(1), 130 (2017)
4. W. Tao et al., Gait analysis using wearable sensors. *Sensors* **12**(2), 2255–2283 (2012)
5. H.Lee, et al., Enzyme-based glucose sensor: From invasive to wearable device. *Adv. Health. Mat.* **7**(8): 1701150 (2018)



6. R. Bouhenguel, I. Mahgoub, M. Ilyas, Bluetooth security in wearable computing applications, in *2008 international symposium on high capacity optical networks and enabling technologies*, (IEEE, 2008)
7. C. T. Hager, S. F. Midkiff. in *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003*. An analysis of Bluetooth security vulnerabilities. Vol. 3. IEEE, 2003. [21] “The Internet of Things and Healthcare Policy Principles.” *2014 Intel*
8. M.N. Islam, M.R. Yuce, Review of medical implant communication system (MICS) band and network. *Ict Express* **2**(4), 188–194 (2016)
9. S. Xu et al., Soft microfluidic assemblies of sensors, circuits, and radios for the skin. *Science* **344**(6179), 70–74 (2014)
10. P. Kumar, H.-J. Lee, Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* **12**(1), 55–91 (2012)
11. D. Sathya, P.G. Kumar, Secured remote health monitoring system. *Health. Technol. Lett* **4**(6), 228–232 (2017)
12. A.D. Dwivedi et al., A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **19**(2), 326 (2019)
13. F. Firouzi et al., Keynote paper: From EDA to IoT eHealth: Promises, challenges, and solutions. *IEEE Trans. Comp-Aid. Des. Integr. Circuit. Syst* **37**(12), 2965–2978 (2018)
14. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 4.5.2016, p. 1)
15. H. Umemuro, Lowering elderly Japanese users’ resistance towards computers by using touchscreen technology. *Univ. Access Inf. Soc.* **3**(3), 276–288 (2004)
16. G. Andreoni, C.E. Standoli, P. Perego, Wearable monitoring of elderly in an ecologic setting: The SMARTA project. *Proc. Sensors Appl* (2015)
17. G.M. Bertolotti et al., A wearable and modular inertial unit for measuring limb movements and balance control abilities. *IEEE Sensors J.* **16**(3), 790–797 (2015)
18. A. Reddy et al., The pH of beverages in the United States. *J. Am. Dent. Assoc.* **147**(4), 255–263 (2016)
19. A.U. Alam et al., Polymers and organic materials-based pH sensors for healthcare applications. *Prog. Mater. Sci.* **96**, 174–216 (2018)
20. M. Al Rasyid, U. Harun, F.A. Saputra, A. Christian, Implementation of blood glucose levels monitoring system based on wireless body area network, in *2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, (IEEE, 2016)
21. T.N. Gia et al., IoT-based continuous glucose monitoring system: A feasibility study. *Procedia Computer Science* **109**, 327–334 (2017)
22. G. Vallathan, A. John, C. Thirumalai, S. Mohan, G. Srivastava, J.C. Lin, Suspicious activity detection using deep learning in secure assisted living IoT environments. *J. Supercomput.* **30**, 1–9 (2020)
23. P.K. Maddikunta, G. Srivastava, T.R. Gadekallu, N. Deepa, P. Boopathy, Predictive model for battery life in IoT networks. *IET Intell. Transp. Syst.* **14**(11), 1388–1395 (2020 Jul 15)
24. Z. Wang, D. Wu, R. Gravina, G. Fortino, Y. Jiang, K. Tang, Kernel fusion based extreme learning machine for cross-location activity recognition. *Inform. Fusion.* **37**, 1–9 (2017)
25. G. Fortino, A. Guerrieri, F. Bellifemine, R. Giannantonio, Platform-independent development of collaborative wireless body sensor network applications: SPINE2, in *2009 IEEE International Conference on Systems, Man and Cybernetics*, (IEEE, 2009), pp. 3144–3150
26. G. Fortino, A. Guerrieri, F.L. Bellifemine, R. Giannantonio, SPINE2: Developing BSN applications on heterogeneous sensor nodes, in *2009 IEEE International Symposium on Industrial Embedded Systems*, (IEEE, 2009), pp. 128–131
27. S. Iyengar, F.T. Bonda, R. Gravina, A. Guerrieri, G. Fortino, A. Sangiovanni-Vincentelli, A framework for creating healthcare monitoring applications using wireless body sensor networks, in *Proceedings of the ICST 3rd International Conference on Body Area Networks*, (2008), pp. 1–2

28. C. Ma, W. Li, R. Gravina, G. Fortino, Posture detection based on smart cushion for wheelchair users. *Sensors* **17**(4), 719 (2017 Apr)
29. C. Savaglio, P. Pace, G. Aloï, A. Liotta, G. Fortino, Lightweight reinforcement learning for energy efficient communications in wireless sensor networks. *IEEE Access*. **7**, 29355–29364 (2019)

# A Fog-Based Intelligent Secured IoMT Framework for Early Diabetes Prediction



Dukka Karun Kumar Reddy, H. S. Behera, Janmenjoy Nayak,  
Ashanta Ranjan Routray, Pemmada Suresh Kumar, and Uttam Ghosh 

## 1 Introduction

One of the chronic metabolic disorders swiftly mounting health catastrophes of this period, irrespective to the context of the ethnic, racial, and geographic situation, is diabetes mellitus. The metabolic disease is characterized by exalted levels of blood sugar (or blood glucose), which leads over time to serious mutilation to the blood vessels, nerves, eyes, heart, and kidneys. In general, diabetes is categorized into three types, called type 1, type 2, and gestational diabetes. Type 1 (is also described as insulin-dependent) occurs where the pancreas produces no insulin or little by itself due to the pancreatic beta cells which have been attacked by the immune system mistakenly. The most common type 1 diabetes symptoms are sudden weight loss, polyphagia, polydipsia, and polyuria. The type 2 diabetes develops when

---

D. K. K. Reddy

Department of CSE, Dr. Lankapalli Bullayya College of Engineering, Visakhapatnam, AP, India

H. S. Behera

Department of Information Technology, Veer Surendra Sai University of Technology, Burla, India

J. Nayak (✉)

Department of Computer Science and Engineering, Aditya Institute of Technology and Management (AITAM), Kotturu, AP, India

A. R. Routray

Department of I & CT, Fakir Mohan University, Balasore, Odisha, India

P. S. Kumar

Department of CSE, Aditya Institute of Technology and Management (AITAM), Kotturu, AP, India

U. Ghosh

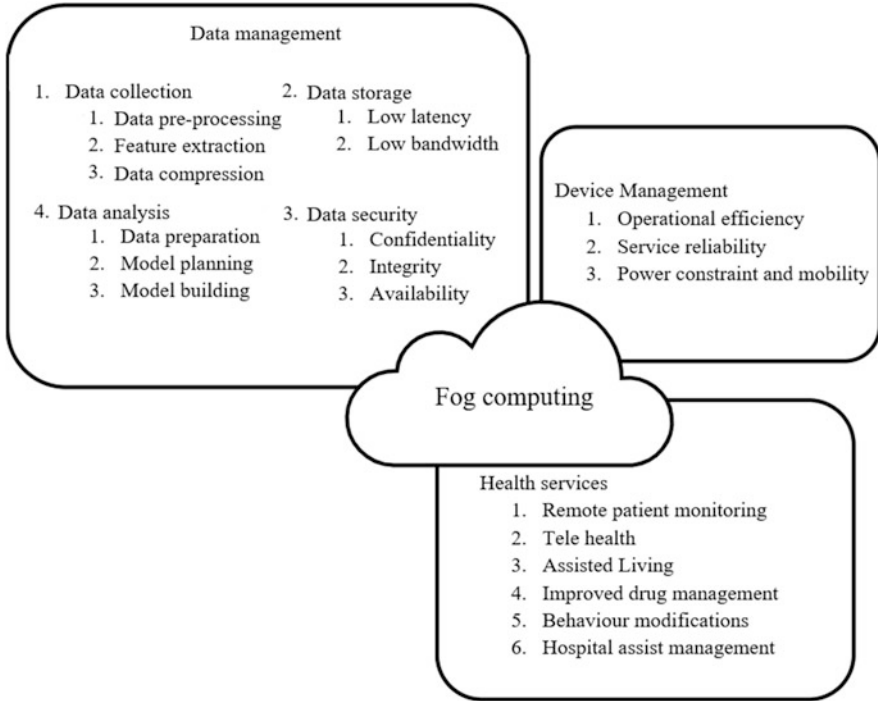
Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA

e-mail: [uttam.ghosh@vanderbilt.edu](mailto:uttam.ghosh@vanderbilt.edu)

the body does not produce enough insulin or becomes insulin resistant. The most common type 2 diabetes symptoms are weakness, delayed healing, and obesity. Third, gestational diabetes is affected by means of hormonal imbalances, only at the pregnancy time, and carries a long-term risk of type 2 diabetes. The other general symptoms of diabetes are blurred vision, extreme hunger, increased thirst, irritability, fatigue, and frequent urination [1]. The prevalence of global diabetes in 2019 is assessed to be around 463 million people (9.3%), which is mounting to 578 million people (10.2%) by 2030 and to 700 million people (10.9%) by 2045. The prevalence in rural areas is 7.2% and high in urban areas with 10.8%. Similarly compared to low-income nations, it is 4.0% and 10.4% for high-income nations. 50.1% of people, i.e., one in two people with diabetes, may not recognize that they have diabetes [2]. Diabetes shows a significant economic consequence, and its complications impose the countries health systems on families and individuals. The effect of diabetes is most directly felt by people living with diabetes and their families, often through loss of family income and for the expenses of diabetes treatment. Artificial Intelligence and Intelligent Technology can help us reliably diagnose such diseases in this new age of technology and can save time and money.

The IoT was coined in 1999 by Kevin Ashton as a groundbreaking paradigm. This technology connects a wide group of devices and objects to interact with each other without human intervention. The main concept behind IoT is to emphasize the relation between reality and the physical world through the Internet [3]. IoT provides a wide range of solutions, for agriculture, smart cities, emergency services, and logistics and transport for the requirements of everyday life [4]. Furthermore, among several other real-life domains, the most attractive areas for IoT applications are the healthcare industry. The legitimate business value facilitated by the fog is extracted from the insights to encourage the real-time behavior that improves asset performance, consistency, and utilization but not really from the data. In order to establish a cross-industry approach to facilitate end-to-end IoT deployments, the fog architecture is coordinated by developing a reference to drive interoperability between the cloud and the edge. With the swift advancement in customized healthcare applications, smart devices, and wireless technology, IoT produces an immense volume of medical and healthcare data. This immense volume of data may be of various kinds such as multimedia, image, and text, which the cloud server requires to store, process, and analyze. The management of cloud with huge medical data contributes to high network traffic and high latency and derives to security problems. Fog computing has emerged as a one-stop solution for both cloud and grid computing limitations. It has proved to be more resourceful to cut down the operational costs by off shoring their data centers to third-party services with distributed computing, data preprocessing, local data analytics, no hidden costs, low network traffic, low network latency, decentralized storage, temporary storage, and effective security and privacy [5].

Health monitoring systems with IoMT-based applications are required with a centralized storage (cloud server) and distributed fog architecture to efficiently perform data analytics. Smart wellness, remote patient access, and ambient assisted living in the healthcare sector can be reaped by using fog computing health system in real time [6, 7]. Fog computing is proved to be very useful for an area where



**Fig. 1** General health services provided by the fog layer

real-time computing plays an essential role in healthcare applications because of processing large amounts of data for time-sensitive applications. Data will have to be processed very quickly and effectively, and the response time will have to be short with enhanced decision-making in the clinical sector with decreased duplication of diagnostics. Fog-based healthcare innovations with enabled devices unleash the ability to keep and maintain patients safe and secure, and inspire doctors to provide the best treatment. Fog facilitates the continuity of healthcare services for a patient status progress update and for those who need real-time regular medical monitoring. Fog architecture accelerates the detection of early diseases and promotes the process of diagnosis and treatment, such as chronic disorders, exercise services, and elderly care, as interactions with doctors have become more effective and simpler, with increased patient involvement and satisfaction. In addition, remote patient health monitoring tends to avoid readmissions and reduces the duration of hospital stay. Fog computing has a significant effect on dramatically lowering healthcare costs and improving the results of therapy. Without a question, fog computing is changing by redefining the space of the healthcare industry, through interaction between people and devices in the delivery of healthcare solutions [8] as shown in Fig. 1.

The IoMT with fog-based healthcare architecture has applications that support patients, families, doctors, and hospitals. For *fog for patients*, wearables such as exercise bands and other wirelessly linked devices provide personalized attention

to access patients with wearable biosensors (e.g., glucometer, heart rate tracking, blood pressure monitoring, etc.). These devices can be configured to remind of blood pressure variations, workout checks, calorie count, appointments, and much more. By allowing such devices, constant monitoring of health conditions has altered the lives of people, particularly aged patients. This has a huge effect on individuals and their families living alone. The warning system sends notifications or messages to healthcare providers and family members worried about any interruption or changes in a person's regular activities. For *fog for physicians*, by using IoT-embedded wearable biosensors and other home monitoring systems, physicians can more reliably monitor the health of patients. They will control the adherence to the patient's treatment or any need for emergency medical care. This encourages clinicians to be more attentive and proactively engage with patients. The fog architecture manages and stores the data gathered from IoT devices for data analysis and helps clinicians to determine the best patient care process and produce the desired results. For *fog for hospitals*, there are several other fields of IoT devices with fog architecture for supportive role play in hospitals, apart from monitoring the health of patients. Sensor-tagged IoT devices are used to track the location of medical devices such as oxygen pumps, defibrillators, wheelchairs, nebulizers, and other monitoring equipment in real time. It is also possible to analyze the deployment of medical personnel at various locations in real time. A significant problem for patients in hospitals is the spread of infections. IoT-enabled systems for hygiene monitoring help to prevent patients from being infected. Fog architecture also assists in asset management, such as control of pharmacy inventory and environmental monitoring, such as temperature control of refrigerator and control of temperature and humidity.

The proliferation of fog architecture is unique to healthcare and provides enormous opportunities. The vast volume of data produced by the allied devices holds the potentiality for the transformation of healthcare. The general IoT healthcare-based architecture essentially contains a four-step process. Sequentially, all four stages are related so that data is obtained or processed at one stage and gives the value to the next stage. Integrated principles in the process have intuition and dynamic prospects for the healthcare sector.

---

#### General fog healthcare-based architecture

---

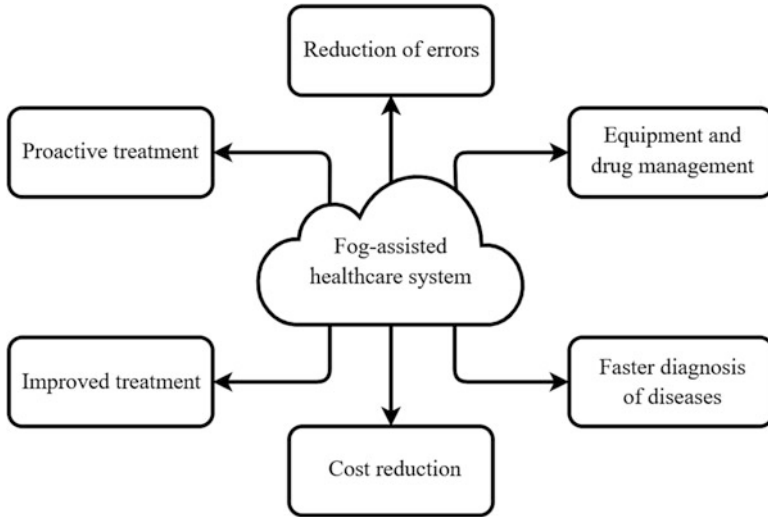
Step 1: The first step is to deploy the interconnected devices containing sensors, camera systems, detectors, actuators, etc. through which data is obtained

Step 2: The sensors and other devices receive the data in analog form and transferred with aggregated and digitized form to the fog architecture

Step 3: This digitized data is standardized, preprocessed, and compressed with feature extraction, where the data is analyzed effectively with data preparation, model planning, and model building

Step 4: Ultimately, at the required level, the data is managed and analyzed. Applied to this info, advanced analytics brings measurable insights for successful decision-making

---



**Fig. 2** Fog-assisted healthcare system with patient's overall satisfaction

Figure 2 shows the major advantages of fog computing in healthcare including patient overall satisfaction through various treatments such as:

- (a). *Improved treatment*: it helps the clinicians to make appropriate informative evidence-based choices with complete transparency on facts.
- (b). *Proactive treatment*: regular monitoring of well-being opens the door to proactive medical care.
- (c). *Reduction of errors*: information produced by IoT devices not only serves to create successful decisions and provides easy healthcare processes with condensed system costs.
- (d). *Equipment and drug management*: in the healthcare industry, medical equipment and drug management is a major challenge. These are controlled and used competently with reduced costs through linked devices.
- (e). *Faster diagnosis of diseases*: the real-time data (constant monitoring) of patients helps to diagnose the symptomatic progression of the disease.
- (f). *Cost reduction*: IoT solution enables real-time patient monitoring, thus greatly reducing unnecessary doctor visits, readmissions, and hospital stay.

With all the advantages, IoMT application is accompanied by the possibility of vulnerabilities and new security breaches in the healthcare system. This is correlated with the following factors: (1) as medical devices mainly capture and exchange confidential patient data, (2) IoT technology design causes complexity and incompatibility issues and, (3) production companies of medical IoT systems do not pay attention to security features. Major security concerns such as confidentiality, integrity, and availability are increasing due to the abovementioned variables. These are necessary to enforce apt security steps. Fog architecture is redefining

healthcare by healthier processes and workflows, with safeguarding, improved clinical outcomes, decreased patients' costs, and satisfactory patient experience from healthcare providers.

The main contribution of this chapter:

- (i) Design and implementation of ensemble GB approach in a fog environment
- (ii) Assessing the influencing features of diabetes disease for fog-assisted healthcare system to understand and make it competent for feasible consequences in detecting prediabetes signs
- (iii) Effective study of performance analysis with proposed method and other competent machine learning (ML) algorithms
- (iv) Examining the performance using the metrics such as F1-score, recall, precision, accuracy values, ROC, DET, and precision-recall curve

Compared to ML classifiers, the predicted model has a robust impact on diabetes classification. The chapter is systematized as follows: Section 2 presents a brief analysis of significant work in the diabetes field. Section 3 describes the GB proposed technique with various ML algorithms for the data analysis part. Section 4 presents the description of the dataset and performance metrics. Section 5 demonstrates the experimental configuration and result analysis. Section 6 presents the conclusion.

## 2 Literature Review

The early diabetes prediction with the assessment of symptoms is receiving more significance and attention. Subsequently, the periodicity of diabetes patients is rapidly increasing. The examination of prediabetes will play a considerable challenge for early assessment of diabetes. The ML technique has been a significant inspiration for numerous researchers because of its potential in characterizing and predicting diagnosis of diabetes at an early stage and symptom assessment of diabetes risk. Table 1 shows some of the methodology and comprehension works proposed by various researchers.

## 3 Proposed Method

Ensemble learning is the principle of ML with the progression of several models, used mainly to stimulate the approximation of functions, classification, prediction, etc. Through strategic perspective, these models such as experts or classifiers are developed and combined in solving a particular problem of computational intelligence by producing one optimal predictive model [20]. Boosting is the branch of ensemble learning techniques with one of the most widely used algorithmic calculations in data science. Boosting is another productive way to improve the



**Table 1** Various diabetes prediction algorithmic models

Reference	Dataset used	Proposed method	Comparison method	Metrics	Observation
[9]	National Health and Nutrition Examination Survey dataset	Combination of LR and RF	NB, DT, AdaBoost	Accuracy and ROC	Logistic regression is used for effective attribute (feature selection) on the given diabetes dataset, where seven attribute factors are found to be statistically significant at 5% level and the remaining factors are found to be insignificant for diabetes disease. The RF is used to classify and predict early diabetes
[10]	PIMA diabetes dataset	ML using pipeline	LR, RF, GB, LDA, AdaBoost, ET, Gaussian NB, bagging, DT, MLP, SVC, and k-NN	Precision, recall, F1-score, and accuracy	Initially highly correlated attributes were evaluated on the diabetic dataset which are, age, and glucose. K-means clustering is performed on these two attributes to classify each patient into either a diabetic or nondiabetic class
[11]	PIMA Indian Diabetes dataset	Ensemble of different ML classifiers	k-NN + DT + RF + AB+NB + XB, DT + AB+RF + XB, k-NN + DT + RF + XB + NB, k-NN + DT + XB	Specificity, sensitivity, precision, false omission rate, diagnostic odds ratio, and ROC	The robustness of the best ensemble classifier with sequential (adaptive) and parallel (gradient boosting) is proposed for the diabetes prediction as the best combination. The proposed approach performed well compared to ML algorithms with correlation-based feature selection on the basis of outlier rejection, filling missing value
[12]	PIMA Indian Diabetes dataset	ML algorithms	RF, SVM, and CNN	Precision, recall, F1-score, and accuracy	The proposed model is built on two important parameters that affect the accuracy of RF classifier, which are maximum depth and the number of DT. These parameters are empirically calculated and set to 7 and 20, respectively, through grid search

(continued)

**Table 1** (continued)

Reference	Dataset used	Proposed method	Comparison method	Metrics	Observation
[13]	PIMA Indian Diabetes dataset	ML algorithms	RF, SVM, NB, and simple CART algorithm	F1-score, recall, precision, and accuracy	ML approaches are implemented for early diagnosis of disease prediction and for helping the physicians for effective diagnosis
[14]	PIMA Indian Diabetes dataset	ML algorithms	SVM, k-NN, RF, NB, DT, and LR	TP, TN, FN, FP, and accuracy	The performance of the ML algorithms is evaluated through data preprocessing for missing values in the dataset through imputation. After that feature selection is performed, out of nine features, eight features were selected for training the ML models
[15]	PIMA Indian Diabetes dataset	ML algorithms	NB, SVM, and DT	F1-score, recall, precision, ROC, and accuracy	The study is motivated through various ML algorithms to design a model which can prognosticate the likelihood of diabetes in patients with maximum accuracy
[16]	PIMA Indian Diabetes dataset	ML algorithms	k-NN, DT, and NB	F1-score, recall, precision, and accuracy	The dataset is studied and analyzed for building an effective model for early prediction and diagnosis of diabetes. The work comprises of bootstrapping resampling technique to enhance the accuracy and then applying ML algorithms
[17]	SMBG data	ML algorithms	k-NN, RF, and SVM	Specificity and sensitivity	The hypoglycemia prediction models (model 1.1 and model 1.2) using ML methods for curtailing the existence rate of hypoglycemia in patients with type 2 diabetes. These ML algorithms performed with a high degree of specificity and sensitivity using sparse SMBG data. The models which used medication information had enhanced specificity and reduced FP predictions

[18]	Hospital physical examination data in Luzhou, China	ML algorithms	MLP, DT, and RF	Matthews correlation coefficient, sensitivity, specificity, and accuracy	<p>Diabetes mellitus is a disease which can cause many complications. ML algorithms are used to predict and diagnose this disease. In this study, minimum redundancy maximum relevance and principal component analysis (PCA) are used to reduce the dimensionality. According to the experimental analysis, it is found that accuracy by using PCA is not promising and the results by using all features with minimum redundancy maximum relevance have produced better results</p> <p>The user's symptom is taken as input (dataset) and the best data mining algorithm is chosen to build the model for the end users. The performance of the algorithms was validated with appropriate evaluation metrics, through tenfold cross-validation, and percentage split techniques are used for risk prediction of early diabetes</p>
[19]	Sylhet Diabetes Hospital in Sylhet, Bangladesh	Data mining techniques	RF, DT, NB, J48, and LR	TPR, FPR, precision, recall and F1-score	<p>The user's symptom is taken as input (dataset) and the best data mining algorithm is chosen to build the model for the end users. The performance of the algorithms was validated with appropriate evaluation metrics, through tenfold cross-validation, and percentage split techniques are used for risk prediction of early diabetes</p>

*NB* Naive Bayes, *DT* decision tree, *LR* logistic regression, *RF* random forest, *GB* gradient boosting, *LDA* linear discriminant analysis, *ET* extratrees, *MLP* multilayer perceptron, *SVC* support vector machine, *k-NN* k-nearest neighbor, *CNN* convolutional neural network

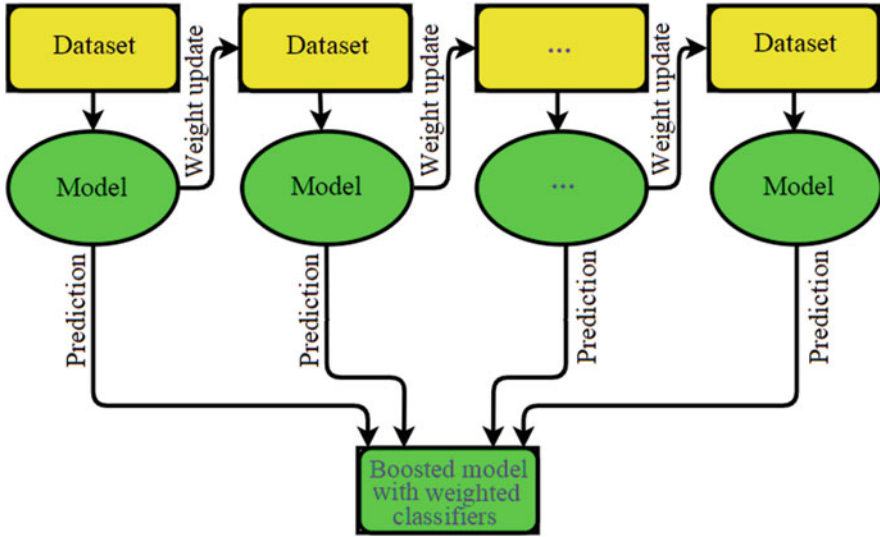


Fig. 3 General boosting technique

predictive control of decision-making for classification and regression models, where a series of weak learners (base learners) are referred to and combined to build a strong learner that achieves better output than a single one. The boosting techniques draw simple learners together to form a powerful structure. The basic ML algorithm is used sequentially with different distributions to define the weak rule and correct its predecessor, which creates a new rule for weak prediction. Every time the base learning algorithm is applied, which will integrate all the previously used weak rules into a single strong prediction rule. This entire iterative process followed by the selection of the correct distribution with copious iterations for each round is commonly known as a boosting technique as shown in Fig. 3.

The GB algorithm involves three major steps for training the model into different submodels, i.e., optimizing the loss function, base learners for predictions to make, and minimizing the loss function. An adaptive model is incorporated with base learners, where each submodel gradually reduces its loss function by using the gradient descent technique [21]. This course of action integrates all the submodels (trees) through successively learning and is provided with a highly accurate prediction for the given variables.

The final output estimation is derived from the integration of all the predictions from various base learners. In GB the base learners are provided with DT. These DTs restrict the nodes of every DT that take different features of the data subset for picking the best split. The submodel reflects on the errors made by the preceding tree, and taking these considerations into account, a consecutive DT's built from preceding trees' errors, by ensemble all the preceding predecessors of DT's model. The model integrates different base learners' predictions to generate the final performance prediction. Figure 4 illustrates the systems overall framework.

Gradient boosting algorithm

<b>Step 1</b>	Initialization of weights to $w : w_1, w_2, \dots, w_n = \frac{1}{n}$ where $n$ be the total instances of the dataset
<b>Step 2</b>	Initialize $f$ with some constant value, where $f$ ensemble function
<b>Step 3</b>	While $m < M$ do: where $M$ is the number of models to be grown
<b>Step 3.1</b>	models are created and get the hypothesis is $H_m(x_n)$ for all data points, where $x_n$ in the dataset and $y_n$ corresponds labels
<b>Step 3.2</b>	computing the negative gradient $\{g_m(H_m(x_n))\}_{n=1}^T$ $g_m(H_m(x_n)) = \left( \frac{\partial \psi(y_n, f(H_m(x_n)))}{\partial f(H_m(x_n))} \mid H_m(x_n) \right)_{f(H_m(x_n)) = f^{m-1}(H_m(x_n))}$
<b>Step 3.3</b>	fitting a new base learner function $h(H(x), \theta_m)$
<b>Step 3.4</b>	calculating the best gradient descent step size $\rho_m$ $(\rho_m, \theta_m) = \arg \min_{\rho, \theta} \sum_{n=1}^T \psi(y_n, f^{m-1}(H_m(x_n))) + \rho h(H_m(x_n), \theta_m)$
<b>Step 3.5</b>	computing $\psi_m$ which is a specific loss function $\psi(y, f)$
<b>Step 3.6</b>	updating the function estimate for model $f_m = f_{m-1} + \rho_m h(H_m(x_n), \theta_m)$
<b>Step 4</b>	Following $M$ iterations, the final regression functional output with $f(x) = \sum_m^M f_m(x)$

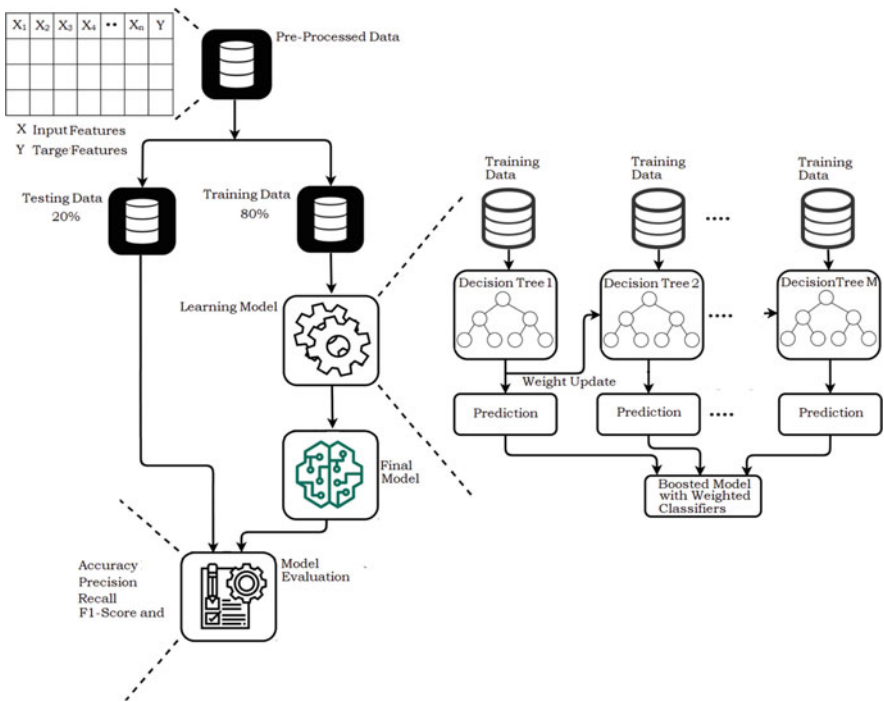


Fig. 4 Overall system framework for gradient boosting

## 4 Materials and Methods

In these sections, the dataset collection and experimental details are discussed. This comprises materials and method of an overall framework for validating the performance measures and results used in the experiment. The dataset collection and observation are the foremost processes of this framework. So, in this process, the collected dataset is observed strictly to find out the types of data. Being a preprocessed dataset and the features consisting of categorical data (Yes and No) is encoded into numeric data. The data feature vectors are sliced through stratified K-fold with five splits as training and testing set (with 80% training data and 20% testing data). The learning algorithms are fine-tuned through parameter setting to develop a final model by using a training set. The ML classifiers employed optimization techniques as gradient descent technique for multilayer perceptron (MLP). Because of nonparametric models, no optimization techniques are used for k-nearest neighbor (k-NN), AdaBoost, and GB classifiers. The complete performance of the model is assessed against testing set with various evaluation metrics.

### 4.1 Dataset Description

The dataset used in our experiment is an early-stage diabetes risk prediction dataset, which is an open-source dataset collected from the UCI repository. This dataset contains the sign and symptom data of the newly diabetic or would-be diabetic patient, and was firstly introduced by MMF Islam et al. [19]. The data is collected through direct questionnaires from Sylhet Diabetes Hospital patients in Sylhet, Bangladesh, and approved by physicians. The dataset furthermore contains 520 total instances with 17 features (age, gender, polyuria, polydipsia, sudden weight loss, weakness, polyphagia, genital thrush, visual blurring, itching, irritability, delayed healing, partial paresis, muscle stiffness, alopecia, obesity, and class) with target feature labeled as Class. The age attribute contains 45 instances within the age group of 11–30 yrs., 123 instances within the age group of 31–40 yrs., 145 instances within the age group of 41–50 yrs., 127 instances within the age group of 51–60 yrs., and 80 instances within the age group of 61–90 yrs. The sex attributes contain 328 male instances and 192 female instances. And the rest of the attribute information contains instances with “yes” (represents blue) and “no” (represents orange), as shown in Fig. 5. The “Class” is the target variable with binary classification, which contains the prediction of diabetes as positive with 320 and negative with 200 instances. The described dataset features are object type except for age, which is int64 datatype.

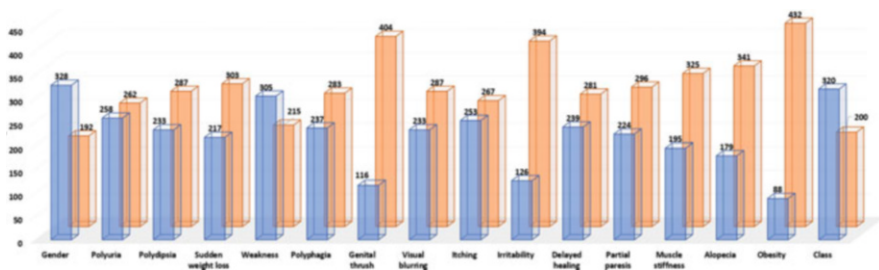


Fig. 5 The dataset attributes

## 4.2 Performance Metrics

To assess the effectiveness of the developed system, performance evaluation aims to estimate the accuracy of the model and also appropriate technique for this work on future data. The confusion matrix gives a clear picture with the types of errors that are being made at classification by false positive (FP), true positive (TP), false negative (FN), and true negative (TN), and exactness of the classifier through true positive rate (TPR) also known as sensitivity or recall (Eq.(1)), false positive rate (FPR) (Eq.(2)), precision (Eq.(3)), F1-score (Eq.(4)), accuracy (Eq.(5)), precision-recall, DET (detection error trade-off), and receiver operating characteristic (ROC) curve will be computed for plotting the TPR with the FPR at different threshold situations:

$$\text{TPR} = \frac{(\text{TP})}{(\text{TP} + \text{FN})} \quad (1)$$

$$\text{FPR} = \frac{(\text{FP})}{(\text{TN} + \text{FP})} \quad (2)$$

$$\text{precision} = \frac{(\text{TP})}{(\text{TP} + \text{FP})} \quad (3)$$

$$\text{F1 - score} = \frac{(2 * \text{TP})}{(2 * \text{TP} + \text{FP} + \text{FN})} \quad (4)$$

$$\text{accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \quad (5)$$

## 5 Experimental Configuration and Result Analysis

The process is evaluated in order to assess the feasibility of this study and visualize the dataset, as any dataset does not show the appropriateness under uncertainty. Undetected cases of phenomena from the dataset are revealed in the experimental procedure and result study. The experimental setup utilized IdeaPad 330LENOVO laptop with the Windows 10 operating system, i5-8250U CPU processor, and RAM size of 8GB. Pandas, NumPy, Scikit-learn, and Matplotlib framework are used for data analysis and information visualization.

In the proposed fog-assisted healthcare system, several physiological conditions of patients, such as blood pressure, glucose levels, body temperature, and physical movements, are continuously monitored and recorded by wearable sensors or through electronic medical records from trusted sources. In order to predict more accurately unusual patterns of the situation, contextual information can also be supplemented with health data. The sensed raw data is then transmitted to the fog layer from various sensors using smart devices periodically. In the intermediate fog layer, functions such as data management (data collection, data storage, data security, and data analysis), device management, and classification of health services are performed. The network layer is used to safely migrate health data across various promised networks from the fog layer to the cloud layer. The cloud computing layer performs statistical patient-centric research through data storage for broadcasting and recommendations for authorized users. Finally, the report visualization, reviews, recommendations, and emergencies are alerted to service providers and end users by message or notification, through mobile or web application.

This result analysis section represents the proposed GB algorithm with traditional ML classifiers k-NN and MLP and with AdaBoost classifiers. Figure 6 shows the confusion matrix of the abovementioned algorithms. The k-NN model predicts 38 instances of negative and 59 instances of positive cases precisely, and the remaining 7 instances are wrongly predicted. The MLP model predicts 38 instances of negative and 61 instances of positive cases precisely, and the remaining 5 instances are wrongly predicted. Only four instances of AdaBoost are wrongly predicted, whereas the proposed method exactly classified the instances of diabetes prediction. The ROC curves for the k-NN, MLP, and AdaBoost produce an area of 0.97, 0.98, and 0.99 for the target diabetes classes of negative and positive. The GB has evaluated with an area of 1.00 for both the classes as shown in Fig. 7. Figure 8 shows the areas of the precision-recall curves for the mentioned models. The k-NN evaluates the area of 0.96 for negative and positive classes. The MLP classifies the positive class effectively when compared to the negative class and gives an average area of precision-recall of 0.986. Similarly, the AdaBoost gives an average area of precision-recall of 0.994. The GB produces an overall average area of 1.00, i.e., the area of precision-recall for both the target classes is 1.00. Figure 9 shows the model's performance with metrics, TPR, FPR, F1-score, precision, and accuracy. The proposed approach gives a TPR, F1-score, and precision of 100% for classification to predict the early symptoms of diabetes with higher classification



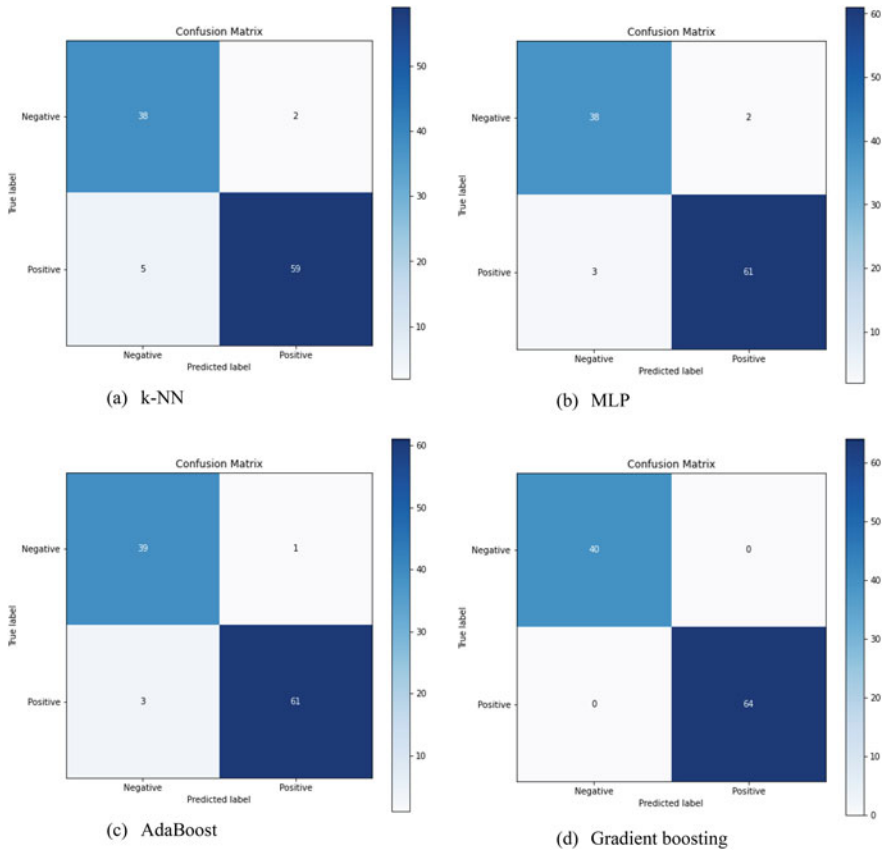


Fig. 6 Confusion matrix analysis

accuracy. Figure 10 shows the overall performance comparison of the models. The DET curves give the detection error trade-off analysis of the abovementioned algorithms.

## 6 Conclusion

The rate of diabetes suffering is increasing day by day, and in the current situation, the healthcare sector is in a great state of desperation. As there is currently no cure for diabetes, IoMT with fog-based health monitoring lays the path for the early diagnosis of diabetes and proper medication at the right time. Fog computing leads a critical role in the process of remote patient health management systems as an intermediate layer. The quality benefit of a health monitoring system can be accomplished by eliminating redundant data and unnecessary communication with

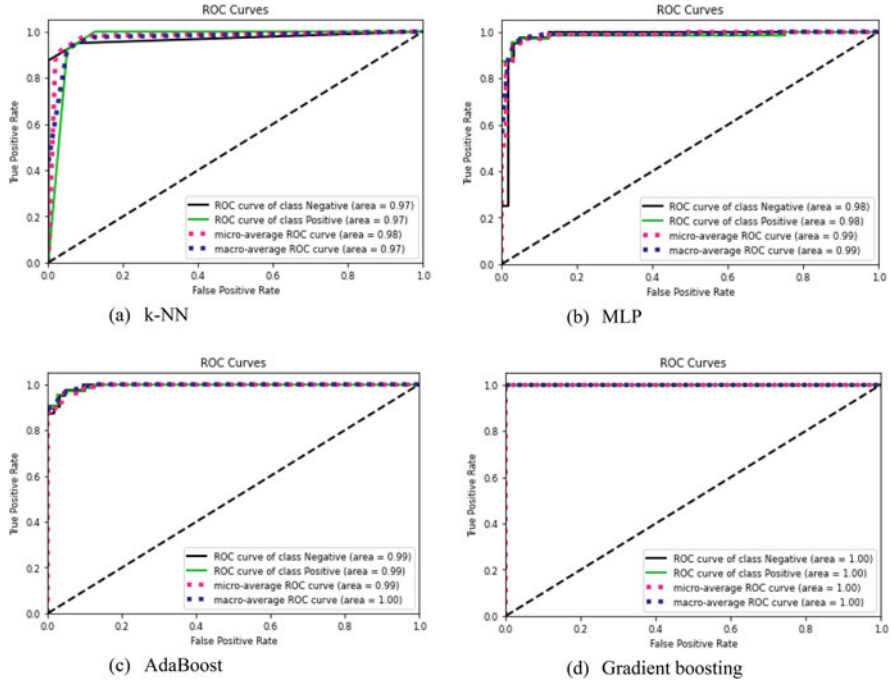


Fig. 7 ROC curve analysis

regard to low network bandwidth and low latency through reduced execution time. The proposed GB classifier makes an effective prediction on the early diagnosis of diabetes with an improved classification accuracy of 100% over other baseline methods on the mentioned dataset. As no novel algorithm is formulated on this dataset, a further study is required for an in-depth analysis for formulating a prototype for new dimensions of medical assistance through a real-time health prediction system and access to patients' health data with improved accuracy and reliability.

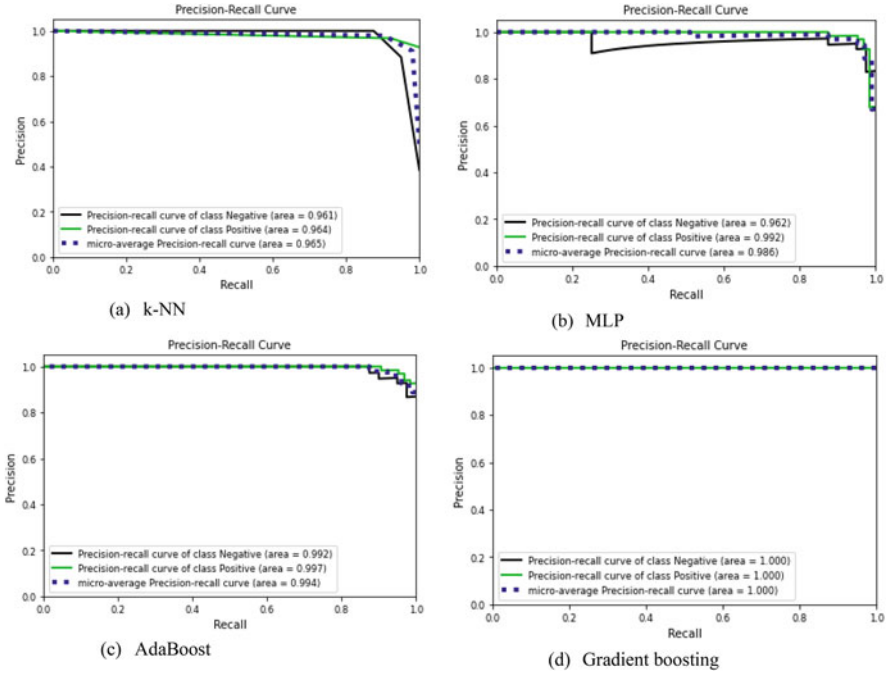


Fig. 8 Precision-recall analysis

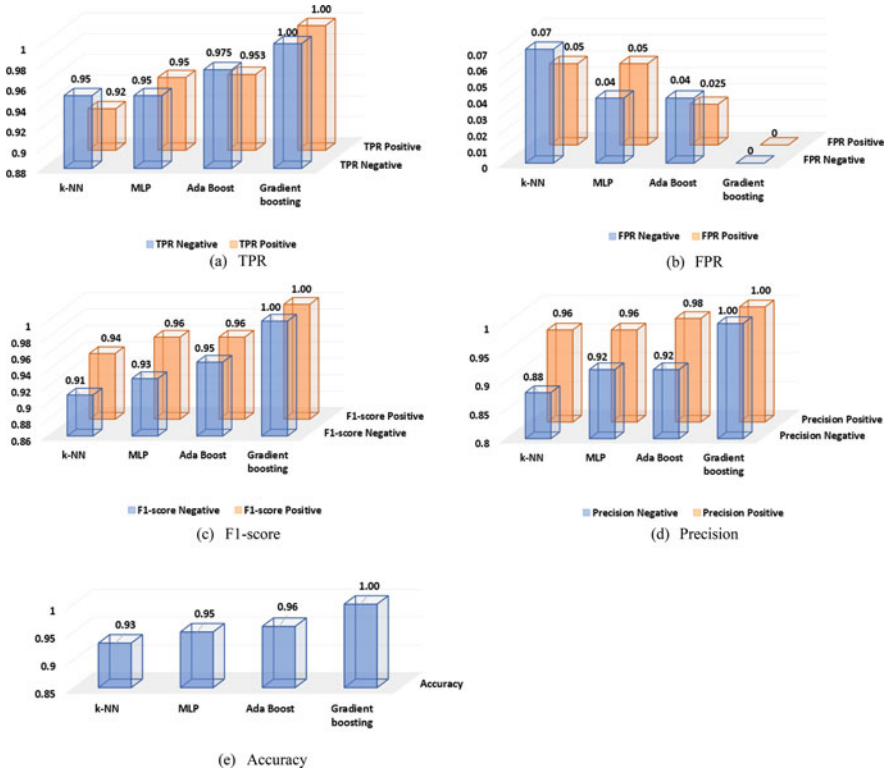
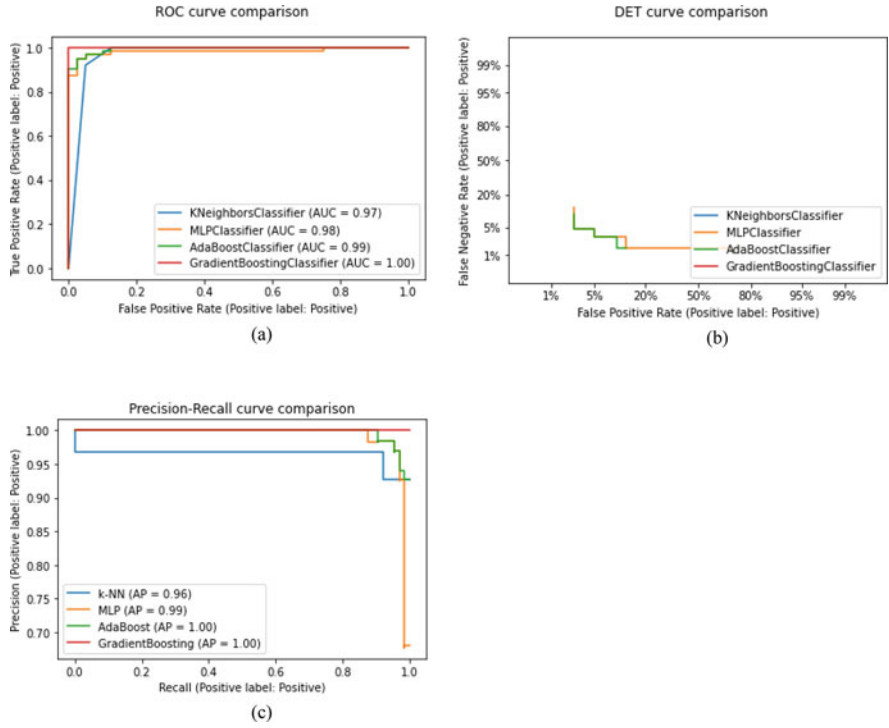


Fig. 9 Overall metrics analysis of all the models



**Fig. 10** Performance comparison of all models (a): ROC curves, (b): DET curves, and (c): Precision-recall curves

## References

1. A. Irani, "Classification of diabetes mellitus," in *PG Textbook of Pediatrics: Systemic Disorders and Social Pediatrics (Volume 3)*, vol. 21, 1, Jaypee Brothers Medical Publishers (P) Ltd., 2015, pp. 2562–2562
2. P. Saeedi et al., Global and regional diabetes prevalence estimates for 2019 and projections for 2030 and 2045: Results from the international diabetes federation diabetes atlas, 9th edition. *Diabetes Res. Clin. Pract.* **157**, 107843 (2019)
3. D.K. Reddy, H.S. Behera, J. Nayak, P. Vijayakumar, B. Naik, P.K. Singh, Deep neural network based anomaly detection in internet of things network traffic tracking for the applications of future smart cities. *Trans. Emerg. Telecommun. Technol.*, 1–26 (2020)
4. P. Singh, A. Nayyar, A. Kaur, U. Ghosh, Blockchain and fog based architecture for internet of everything in smart cities. *Futur. Internet* **12**(4), 61 (2020)
5. OpenFog Consortium Architecture Working Group, OpenFog reference architecture for fog computing. *OpenFog*, 1–162 (2017)
6. A.P. Singh et al., A novel patient-centric architectural framework for Blockchain-enabled healthcare applications. *IEEE Trans. Ind. Informatics*, 1–1 (2020)
7. Y. Sun, F.P.-W. Lo, B. Lo, Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **7**, 183339–183355 (2019)
8. I.S.B.M. Isa, T.E.H. El-Gorashi, M.O.I. Musa, J.M.H. Elmighani, Energy efficient fog-based healthcare monitoring infrastructure. *IEEE Access* **8**, 197828–197852 (2020)
9. M. Maniruzzaman, M.J. Rahman, B. Ahammed, M.M. Abedin, Classification and prediction of diabetes disease using machine learning paradigm. *Heal. Inf. Sci. Syst.* **8**(1), 7 (2020)
10. A. Mujumdar, V. Vaidehi, Diabetes prediction using machine learning algorithms. *Procedia Comput. Sci.* **165**, 292–299 (2019)
11. K. Hasan, A. Alam, D. Das, E.H. Senior, Diabetes prediction using Ensembling of different machine learning classifiers. **X**, 1–19 (2020)
12. A. Yahyaoui, A. Jamil, J. Rasheed, and M. Yesiltepe, "A decision support system for diabetes prediction using machine learning and deep learning techniques," in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, (2019), 2, pp. 1–4
13. A. Mir, S.N. Dhage, Diabetes disease prediction using machine learning on big data of healthcare, in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCCUBEA)*, (2018), pp. 1–6
14. M.A. Sarwar, N. Kamal, W. Hamid, M.A. Shah, Prediction of diabetes using machine learning algorithms in healthcare, in *2018 24th International Conference on Automation and Computing (ICAC)*, (2018), pp. 1–6
15. D. Sisodia, D.S. Sisodia, Prediction of diabetes using classification algorithms. *Procedia Comput. Sci.* **132**(Iccids), 1578–1585 (2018)
16. Y.J.N. Kumar, N.K. Shalini, P.K. Abhilash, K. Sandeep, D. Indira, Prediction of diabetics using machine learning. *Int. J. Recent Technol. Eng.* **8**(5), 1119–1124 (2020)
17. B. Sudharsan, M. Peeples, M. Shomali, Hypoglycemia prediction using machine learning models for patients with type 2 diabetes. *J. Diabetes Sci. Technol.* **9**(1), 86–90 (2015)
18. Q. Zou, K. Qu, Y. Luo, D. Yin, Y. Ju, H. Tang, Predicting diabetes mellitus with machine learning techniques. *Front. Genet.* **9**, 1–10 (2018)
19. M.M.F. Islam, R. Ferdousi, S. Rahman, H.Y. Bushra, Likelihood prediction of diabetes at early stage using data mining techniques, in *Advances in Intelligent Systems and Computing*, vol. 992, (2020), pp. 113–125
20. R. Polikar, Ensemble learning. *Scholarpedia* **4**(1), 2776 (2009)
21. J.H. Friedman, Greedy function approximation: A gradient boosting machine. *Ann. Stat.* **29**(5), 1189–1232 (2001)

# A Comprehensive Analysis of Sustainable IoT Infrastructure in the Post-COVID-19 Era



Deepsubhra Guha Roy

## 1 Introduction

With the increase in worldwide population, the amount of data that needs to be processed is increasing exponentially and efficient mechanisms to store, process and retrieve the data are in high demand. Due to the sudden pandemic caused by COVID-19, several unique challenges have been raised in the society and economy, for which cutting-edge applications are in demand to balance between the increased technological requirements and the restrictions to survive against the disease. To avoid the infection spread, social distancing and lockdown measures have been imposed by countries all over the world, and in this context, our personal and professional life have observed significant changes irrespective of the place and time. Internet of Things-based remote monitoring facilities have been widely adopted by the organizations to facilitate the work from home system and avoid direct contact among employees. Educational institutes have also switched to e-learning platform and medical organizations like hospitals and nursing homes are also implementing remote patient monitoring and e-medicine where some people have been benefited and some have been deprived also due to technological bound in their circumstances. The digital transformation not only means the adoption of state-of-the-art technologies, but also the strategic decision about the modified business approach where payment mechanisms have also changed in the new business models.

Climate change and global warming originated by different types of pollution have been the greatest threat to the world, and feasibility of sustainable infrastructure [1] both from environmental and technical aspect have been a point of attraction in this context [2]. If we systematically address the Sustainable Development Goals

---

D. Guha Roy (✉)

Mobile and Cloud Lab, Institute of Computer Science, University of Tartu, Tartu, Estonia



**Fig. 1** Pictorial representation of Sustainable Development Goals

(SDGs) introduced by United Nations [3], many of the current urban problems will get resolved and improvement in the quality of life will be observed eventually. The goals have been illustrated in Fig. 1. They were vital before the crisis era; now they have got integral with our life. Hunger, thirst and energy demands increased since the pandemic [4, 5]. While recovery is unpredictable, interconnected devices and multi-use sensors can lead the way to take the required actions in order to serve the above-mentioned purpose. If IoT is implemented with conscience and care, it may offer a chance to improve the situation for billions of people, trying to survive in the developing countries.

Besides this, digital technologies and innovations have reportedly become societal needs during the lockdown caused by novel coronavirus spread [6]. Many governments have taken modernized digitized defensive strategies to overcome this crisis period. In this difficult situation imposed by COVID-19 pandemic,

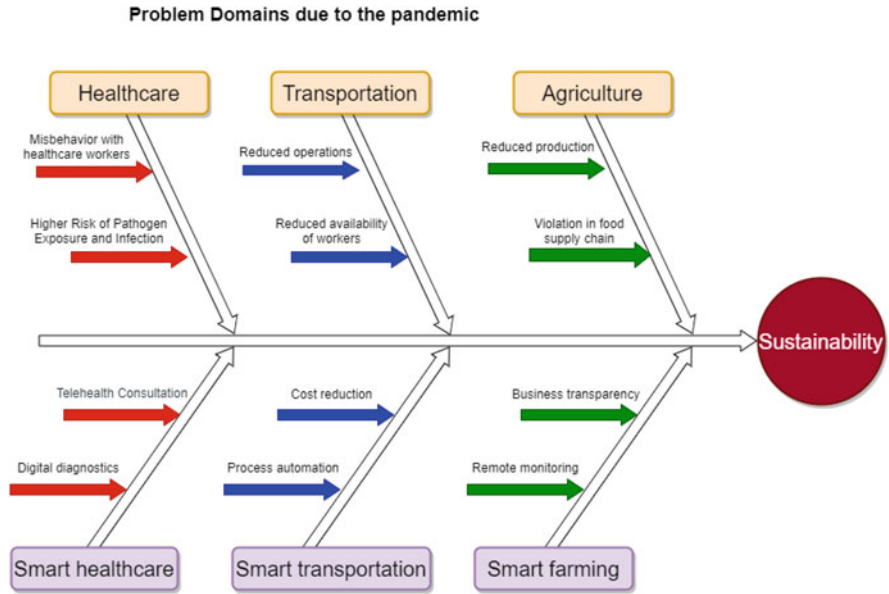


emerging digital technology implementation at large scale in very little time is being demanded by unparalleled humanitarian plus economical needs [7]. For promotion of public health to answer the worldwide spread of novel coronavirus, digitized mechanisms, which include monitoring population, recognition of an event, tracking touch, assessment of action focused on mobility data and engagement with the public, are getting accepted. For minimization of COVID-19 crisis, early detection, patient surveillance and following the protocols after a patient recovers, all these can be done by IoT-enabled/linked applications/devices [8, 9]. Our advanced technology and the integrated position of IoT do have what it takes to defeat COVID-19. On achieving SDGs, Internet of things posed in the developed world would have a huge impact is being believed by some researchers [10, 11]. Digitization and sustainability in effect are key to develop the economy and improve the climate and culture. For promotion of a transition to sustain development phases, the nexus between both domains display an unexposed, yet brilliant possibilities [12]. Although digitized sustainability problems are yet to have a solution [13].

The next section will discuss some related works in the IoT paradigm which have been proved to be sustainable for our environment. Their advantages along with shortcomings will be analysed for further research in the concerned area. In Sect. 3, various application domains of those sustainable IoT solutions relevant to our present situation will be discussed. The last section will conclude the analysis and a possible research direction will be attempted to be identified for a better future.

## 2 Background Study

To prevent problems of environment, that may cause man made or even natural disasters, for preservation of natural resources, many researchers are trying to conduct their work in this domain. Figure 2 describes multiple problem domains, where IoT can resolve these issues in the post-COVID world. De Viliers et al. in [14] stated that all the problems of SDGs are not addressed by IoT technologies and technology-enabled capabilities. Figuring out some barriers systemic or outside the technologies is important. Further direct steps can be driven by equitable and ethical legislation, financial enablers and regulatory outlines. To change the playing ground these are needed. To meet growth and growth targets, developed states should point out creative policy frameworks that are also economical. For example, looking for affordable measures which may result in instant profits in several SDGs, instead of trading those goals for reaching others and adding financial states to grow sustainable in the long run [15]. E-learning system's sustainability for the pandemic period in Romania has been analysed in [16]. Looking from the perspectives of teacher–student–parent, a sustainable and effective learning solution, looking at the present and future days, can be e-learning. But well-collaborated teachers–parents, monitoring behaviour of the younger ones, i.e. the students to find out and fight probable effects, determined by the modified methods of learning and social realities, are required.



**Fig. 2** Problem sectors and probable IoT-based solutions

Various challenges of existing IoT frameworks include resource management [17], delay and message loss [18], high bandwidth consumption [19], privacy and security [20]. For sustainable smart cities, big data applications based on IoT have been reviewed in [21] where mainly two categories of research approaches have been explored, i.e. thematic analysis and topical literature survey. Urban researchers and planners in the concerned area will be benefited from the study as it has given an insight into environmental benefits of using sustainable IoT infrastructure by achieving separate intelligent functions, ranging from conduction of communication and information changes, including planning things, learning about things and repairing them, operating, managing, evaluating, tracing and tracking things, controlling things, identifying things, finding things, monitoring things and connecting with things.

A new sustainable IoT architecture has been introduced in [22] containing five layers, i.e. sensing, interconnecting, platform, interface and business layer meeting the ends between demands and supplies of IoT by bridging public and business values of IoT, plus applications and technologies of IoT. The goal of the platform and business layers discussed in the model is mainly in penetrating the society's lower rank and building trust in IoT products of global market by stricter privacy and security protocols. In [23], a wider range, low cost and low energy based hardware platform of IoT has been introduced for the developing countries of Africa. The sustainability of the model has been tested against three use cases, i.e. waste management, water monitoring at fish pond, water saving at tomato field respectively in Togo, Ghana and Senegal. Reducing the quantity of required water

based on fertilizer, reducing the waste and optimizing the fish growth by monitoring parameters like pH and oxygen, implementing a network of smart waste basket, reducing waste and increasing recycling were the aims of the respective tasks. In parallel with the environmental aspect, societal and economical aspects also have been taken into account to reshape the conventional business sectors. A comparison among six different state of the art in the related area has been presented in Table 1.

To cope up with the requirements associated with sustainable environment, green Internet has been the primary area of concern where the efficient reduction of power consumption in the network system is the main goal [30]. Green IoT is predicted to make huge changes in our future life which will be resulting in green environment with reduced emission of CO<sub>2</sub>, greenhouse effect and pollution hazards. An efficient architecture of green mobile computing has been proposed in [31] where offloading of sensor data to cloud has taken place through mobile device. Home node base station and light weight access point have been applied in the indoor area and microcell and macrocell base stations have been applied in the outdoor area. The power consumption has been reduced up to 10% and 30% in the indoor and outdoor area, respectively. However more efficient mechanisms can be attempted to be applied for improved experimental outcome in the near future. Cloud, edge, fog and grid computing have played vital role in different real-time applications discussed in the latest research papers.

Each technology that is rapidly progressing has got specific potential drawbacks that need to be carefully analysed and addressed. Since IoT devices are measured in billions, and with large potential impacts on the population, specific challenges need to be addressed as discussed in [32] like fast consumption of rare and raw materials, rebound effect of electronic equipment, data acquisition and electronic waste. Two sustainable applications of IoT have been presented in [33] where the first one is for energy and heat management and the second one is for eco-friendly cruise control system using traffic sensors as resource. An air quality survey conducted in the United Kingdom in 2012 mentioned road pollution as two times deadly than traffic accidents since 12% of total CO<sub>2</sub> emissions are from transportation sector and it causes severe health damage [34].

While QoS parameters like scalability, reliability, availability, time, cost and power consumption have been the main focus in the existing literature, there resource utilization, communication overhead, location awareness and interoperability have been a little bit ignored. Thus they can be considered in the future works for better business opportunities [35]. For the sustainable environment concern, creation and application of renewable energy has gained attention from a number of researchers, where blockchain has been widely adopted in green IoT by researchers, financial institutions, business start-ups, governments and energy supply companies [36] for its simplicity, AI-enabled light weight consensus and smart contract, transaction speed and cost. Italy had been the most COVID affected country after China, which resulted in a quick shift to a complete and efficient urban planning practice and model [37]. A spatio-temporal mathematical model has been introduced in [38] to design a self-sustainable IoT paradigm based on queuing theory and stochastic geometry. The IoT framework relies on harvesting

**Table 1** Comparison among state of the art on sustainable IoT architecture

Ref. No.	Objective	Method applied	Outcome	Drawbacks (If found)
[24]	To describe the potential of low power wide area network in real-time scenario for sustainable IoT	Energy neural operation for testing the lab field and adaptive sensor transmission scheduling	Optimization of spectrum, adaptive selection of low power wide area network radio, distribution, sensing without sensors have been identified as the major challenges	Lack of long range low cost connectivity in IoT
[25]	To check the applicability of IoT in sustainable tourism sector in Cagliari city, Italy	Optimized IoT-based route planning model for tourists by selecting right transport and place of interest	55% time saving and 27% greater satisfaction of tourists	No implementation of the actual virtual objects like the queue and traffic sensors and no consideration of user profiling, clustering techniques, cost components' weights based on user choice
[26]	To design an abstract web service gateway for sustainable IoT architecture	Preservation of platform specific optimization as the associated overhead did not offload to the IoT platform	Message-based communication in IoT framework with low run-time overhead and high flexibility	No consideration of sensor network and RFID reader to check the applicability of the gateway design
[27]	To design energy sustainable IoT system having QoS constraints connected to cloud	Multiple Input Single Output (MISO) IoT framework consisting of a multi-antenna Transmitter conducting parallel transmission of information and power to data hungry and low power receivers	The proposed energy harvesting fairness maximization problem performed 20% better than the closest competitor	No consideration of multiple antennas on the IoT platform and array of massive antennas at the transmitter side
[28]	To design an energy-efficient task allocation scheme for mobile cloud-based sustainable IoT	Selection of suitable virtual machine keeping the deadline constraints satisfied in edge data centres	Polynomial execution time reduced the execution delay and energy consumption	No testing of performance in dynamic application platform and practical test beds

(continued)

**Table 1** (continued)

Ref. No.	Objective	Method applied	Outcome	Drawbacks (If found)
[29]	To create sensed data in an intelligent manner and effectively prune that traffic maintaining required QoS	Reliable data transmission in IoT channel satisfying Quality of Protection for sustainable environment	Performance of three IoT applications, namely, smart metering, smart grid health monitoring and lab environment monitoring showed that data-driven green schemes contribute to intelligent computation, communication and sensing	No consideration of effective wireless channel characterization

energy from cellular network, which in turn quantifies the packet delay and the buffer size which are vital for critical IoT architectures. Disjoint spectrum has been allotted to the IoT as well as cellular communication where all the IoT devices have been modelled using a discrete Markov chain which tracks the energy generated at the battery and the chance of successfully transmitting packet from the buffers which in turn have been considered as the performance evaluating parameters of traffic density and intensity in the network.

### 3 Problem Domains

Different challenges experienced by different sectors of our society due to the pandemic will be discussed in this section. In 2015, in its resolution 70/1, the UN General Conference laid out the SDGs with 2030 as its target year [39]. These priorities were established with the involvement of society, including universities, governments and the private sector. It covers three key aspects of sustainable community development (such as environmental protection, communal divergence and inclusion, and monetary development). For reaching the main aim of any community’s sustainable development, the SDGs have become the universally agreed standard method and have been adopted. These priorities are essential in the whole idea of IoT in order to maximize sustainable outline and social impacts [40]. The IoT development generated by COVID-19 has the capacity to address some of the most pressing human, economic and environmental needs. It can also directly contribute to achieving the goals of the SDGs: the evolving IoT paradigm has the ability to use connected devices to create an accessible, efficient and secure environment to manage the major global challenges it and future generations face.

In developed and developing countries, the IoT outline has the important capacity to make significant advances in development and human life [41]. IoT networks with the interconnection of “things” have become easier to form considering the coverage of wireless networks in developing areas. Even though the UN Sustainable Development Goals (SDGs) have been severely illustrated in the diplomatic fallout of COVID-19. They were significant before the pandemic; now they are integral. Hunger, thirst and energy requirements have only become even more pronounced in the decline since the pandemic [42, 43]. Actions should be followed having connected devices and multi-use sensors providing a way to accomplish these efforts in the face of unpredictable recovery. When carefully and conscientiously applied, recent IoT growth offers an opportunity to change the destiny of billions for the better in developing regions.

Ending hunger, achieving food security and raising health literacy are critical societal obstacles that have been alleviated by the current pandemic [44]. Global farming will need more room for more mouths to feed if left unchecked. In an effort over the next decade to produce larger volumes of higher quality food, the UN is also pushing for organic farming. Smart farming is a step towards making this a possibility at this stage, backed by the IoT’s strength. It is anticipated that IoT-based smart farming can yield two major betterment in standards for food processing and data-based automation. New agricultural technology will make farmers more sustainable and automate the crop or animal production cycle, potentially leading to more food at lower prices for the ever-growing population in developing regions. Furthermore, if SDG 2 were to be reached, our food production would also need to be: inclusive, healthy, efficient and nutritious. The task for ICT technologies such as IoT is to ensure the involvement of stakeholders in food systems (economic and social, large and small, women and youth), to mitigate adverse environmental impacts and to have plenty of healthy and safe foods [45].

For billions of people, access to clean water and sanitation is still insufficient, despite some changes. Current inequalities in access to the basic necessities of life create layered vulnerabilities to COVID-19 as clean water and sanitation systems and can render prevention initiatives ineffective or potentially counterproductive [46]. Stakeholder organizations are converging to explore how emerging technologies can deal with water and sanitation issues. In this sense, in conjunction with Big Data Analytics (BDA), IoT sensors can, by automation and remote control, provide efficiencies not just in agriculture but also in sewerage network monitoring so that waste is properly disposed of. In terms of SDG 6, fresh innovations like IoT would provide everyone in developed countries with water and sanitation in an equal manner. Wind, solar, hydropower, geothermal electricity and biomass supplies are growing in the general change away from fossil fuels, and connected devices accelerate efficiency and automation in this transformation [47].

IoT combines all the elements of power generation and usage, enhances operation visibility and provides real control at every point of the energy flow [48]. Sensors and connected devices allow organizations to access real-time energy data for automated storage and analysis and send it to the power grid. Automation is highly important when it comes to generating green energy. Meanwhile, better

load management is feasible because of new insights on voltage modulation, load balancing and network tuning. In the wind, for instance, or solar IoT devices may identify the most favourable conditions of energy production and automatically change the direction of turbines or panels. The use of devices and their data to track and control these power generators efficiently makes it possible for optimal efficiency to maximize power generation and reduce operating costs. Via smart monitoring and management of plants for the development of green energy and smart manufacturing using circular economy objectives, innovative infrastructure such as IoT supported programs achieve SDG 7 efficiently [49].

### ***3.1 Healthcare***

The area which has been affected mostly by the outbreak is the health care [50]. With the impetuous spread of COVID-19, hospital structures had to reorganize the assistance activities and hospital networks for handling the health emergency sometimes within a few minutes or hours and sometimes a few days. They started to convert some of their general wards into intensive, sub-intensive and inpatient regions to accommodate the ever increasing number of patients.

### ***3.2 Transportation***

COVID-19 has affected transport section more than almost any other sectors. From rickshaw pullers to airlines, all are going through financial crisis, as due to lockdown, public transportation systems were least used. The protocols issued by the respective government and even after unlock started taking place, the scare among common people has had a short-term mixed effect when it came down to the demand of transports. On the one hand, to deliver essential goods the demand of truck drivers has increased whereas to prevent air pollution, use of diesel oriented vehicles are getting prohibited, simultaneously, hydrogen-based vehicles' demand are increasing as their alternatives. These are altering the shape of transportation frameworks in future.

### ***3.3 Manufacturing***

Manufacturers have experienced different challenges and chances such as manufacturing investments, transparency, manufacturer staffing, manufacturing supply chains and industrial disaster recovery since the growth in economy after the slowdown due to pandemic. The main four challenges lie in the uncertainty in global spread and duration of the pandemic, disruption of demand and supply sector of

supply chain in the entire world, increasing lead time, little supply inventory and little slack in the supply chain.

### **3.4 Agriculture**

The pandemic has introduced social distancing among people which in turn leads to immediate challenges to the farms and to confirm a sustainable food system, suggests mitigation measures in post-COVID era. For farmers, state-wise protocols have been issued, which must be maintained during lockdown. The guidelines mention typical practices for harvesting and threshing of different winter sown crops, called rabi crops. It also provides post-harvest instructions for storing and marketing farm products. In spite of following these rules and restricting movements of both vehicular and man traffic, related to the negative implications of this outbreak on the finance of farms, raised concerns [51]. The workers crucial for both harvesting and post-harvesting handling of products in marketing and storage organizations started migrating from few parts to their native states, which triggered panic buttons [52, 53].

## **4 Internet of Things-Based Solutions for Smart Sustainable City**

IoT solutions encompass everything IoT device designers, software developers and product manufacturers need to develop and implement IoT ideas, including hardware IP and software platforms. Efficient processor designs combined with AI-enhanced intelligence, end-to-end security, development platforms and tools for multiple workloads, devices and clouds, and massive scalability are all essential elements of an IoT solution. IoT solutions help build massive networks of IoT devices, reducing the complexity, ensuring device efficiency and driving innovation across industries looking for growth opportunities and operational efficiencies. In this section, we will get an overview of the foundations of IoT solutions that are transforming today's businesses. The main focus of smart city concept was to improve the quality of life for residents. The present situation has profoundly tested the applicability of smart city concept in terms of its ability to mitigate the global effects of the sudden pandemic. Cities that would be considered as "smarter" will be having an established crisis operations centre, a plan for resiliency, a plan for preparedness basically connected with a number of crisis-based real-time data acquisition equipment like cameras and sensors. A possible outline of such type of framework has been shown in Fig. 3.

Smart City Blueprint generated by Hong Kong in 2017 draws a brief outline of its aim of making the city more competitive, resilient, sustainable and livable, and



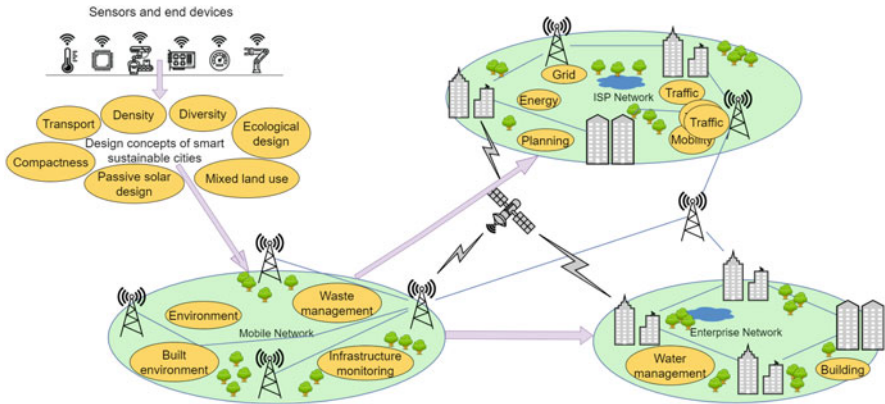


Fig. 3 IoT-enabled smart sustainable city framework

various steps for digitization have been followed where the rest of the metropolitan cities are only planning of taking them into account during the present crisis [54]. Seoul declared their plan of investing 1.2 billion USD in 18 different smart city implementation plans in 2017 involving 50,000 plus sensors of IoT. Infrared thermal checking has been mandatory at airports in most of the countries globally. The Severe Acute Respiratory Syndrome (SARS) experience shaped the preparedness and helped Taipei, Singapore, Seoul, Hong Kong and many other smart metropolitan in planning some probable future actions more quickly and efficiently during the outbreak. It has been observed that activity monitoring, tracing and tracking in different entire cities have been a vital factor of success in this situation.

### 4.1 Smart Transportation

Recently, the COVID-19 pandemic caused half of mankind to suffer an unprecedentedly lengthy lockdown. This has, of course, taken mass transit networks to a complete standstill, resulting in a dramatic decrease in greenhouse emissions and air pollution levels in the impacted regions. Although the health and economic crisis that has been caused still lasts longer and impacts much more than actual expectation, questions emerge as to what this entails for everyday life, urban planning and communication for the future. In particular, a post-COVID-19 city may experience a steady demand drop for commuter transport because of a mixture of a continuing economic recession and shifting work habits. With respect to cramped areas, and public transit in particular, there may be a behavioural shift [55]. Figure 4 has described different possible components of a smart transportation system where location awareness, network scalability, inter-operability, response and delay time minimization are the Quality of Service (QoS) requirements of the systems.

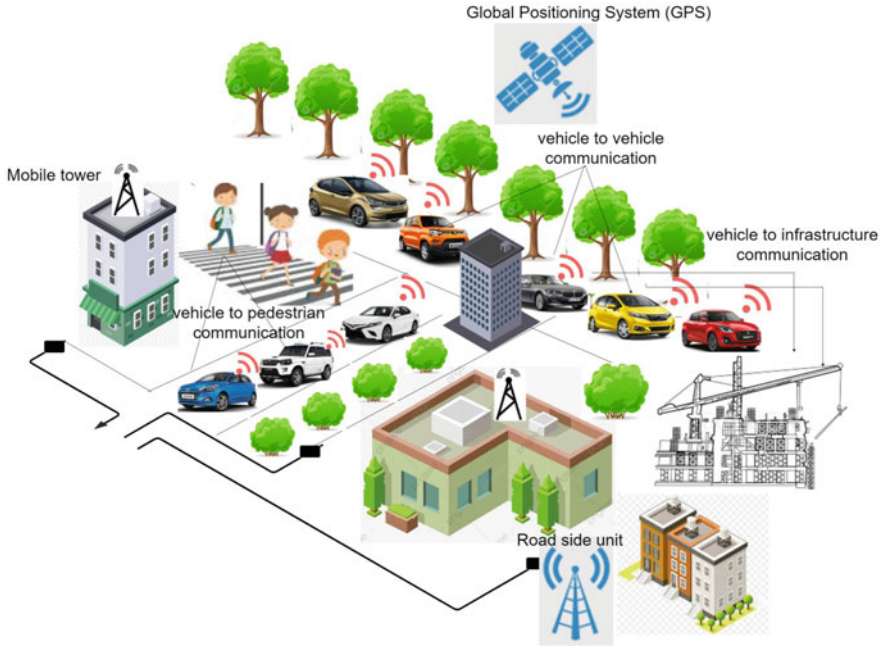


Fig. 4 An overview of smart transportation system

Transportation sustainability means not only handling green transport but also developing successful transport planning frameworks to ensure the safety of road transport. Analysis of statistics [56] has proved that the use of vehicles, especially cars, has been on the rise since 2006. If the condition of weather and the road surface can be assessed along with achieving the sustainable characteristics, road side accidents can be prevented and collisions among vehicles would be controlled also. A comparative analysis among different intelligent transportation systems has been presented in [57] where smarter utilization of autonomous vehicles like self-driving cars will help us to obtain safer, easier and more sustainable transportation. While the usage of non-renewable energy in green transport has been limited, a few considerations remain to be addressed, such as charging systems for electric batteries and prepaid plug-in charging stations. As a common basis for vehicles created by different firms, novel standard charging stations need to be established.

In order to achieve pollution-free travel, the use of electric cars has to be followed by a study of the traffic movement of all kinds of vehicles. Collision avoidance systems in connected cars play a crucial role in ensuring the safety of passengers/drivers during driving, from another perspective. To avoid unnecessary collisions between connected vehicles various other innovations, including image recognition, vehicle prediction, sensor implementation, human behaviour/dynamics analysis and driver response time, and swarm-inspired models are used. Wang et al. have identified some issues in complex systems like transportation, ecosystem

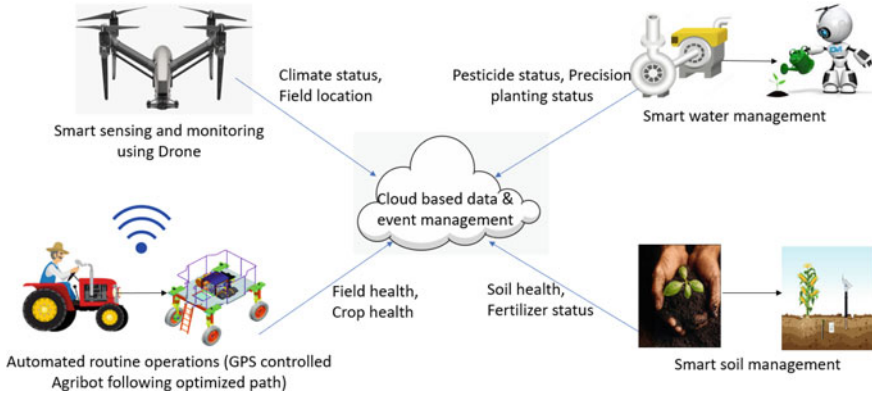


Fig. 5 An overview of smart farming

and logistics where the lack of efficient analysis and modelling method has been detected as the key challenge in the existing works [58]. The second issue as identified by them is the experimenting problem. And the third one is decision-making problem which can be addressed in the future computational strategies and experiments in the transportation sector.

## 4.2 Smart Farming

Despite of several challenges faced by agriculture system due to COVID-19, many new opportunities have been enabled also since its integration with artificial intelligence leading to automation. After the pandemic, the precision farming demand is expected to expand in the long term, as it enables the condition of the crops to be tracked despite not being physically present by the use of automation, reducing the need to contact other people, which is very vital in this situation [59]. This is a method where, opposed to conventional cultivation methods, inputs are used in specific quantities to get improved average yields. However, COVID-19 impacted the industry in the short term and the growth of the market was comparatively sluggish in the first and second quarters of 2020 due to the global downturn and inflation. An overview of the smart farming concept has been shown in Fig. 5.

The outbreak was a never seen before incident which explored uncovered interconnections and inter-dependencies between economy, society and agriculture, while the susceptibility of agri-food production to external disruptions was also brought to the fore. Three future mechanisms that can alleviate the consequences of vital emergencies or agricultural disasters, drawing on the current situation: resilience-promoting initiatives, cooperative marketing schemes and smart farming technologies. We contend that resilience-promoting polices, smart precision

technology, and group promotion schemes. Here is the conclusion of increasing the concentration of resilience-promoting techniques on implementing disaster response strategies and improving the ability of farmers to deal with external disruptions. We also emphasize the requirement of encouraging community marketing activities that provide farmers with an income floor while promoting customer access to agri-food products in parallel allowing customer access to it as they are under-served by conventional delivery networks. Finally, we explore several problems that require an assurance that big data-based smart technologies can assist farmers cope with extrinsic shocks [60].

These activities save time and costs: reducing the expense of fertilizer and pesticide application, reducing emissions by using chemicals less. They often assist in tracking the physio-chemical conditions of the soil and plants: by positioning sensors to calculate parameters such as electrical conductivity, nitrates, temperature, evapo-transpiration, radiation and humidity of the leaves and soils, so that the optimum conditions are reached. Under this pandemic scenario where there is a lack of labour, these aspects help to achieve a higher production with restricted labour force and hence help in the daily supply of food, thus maintaining food stability [61].

### **4.3 Smart Healthcare**

Health care is the one sector that is now embracing multiple IoT strategies to alleviate the strain for its staff as well as to deliver the requisite support to patients fast. The most useful IoT applications in health care, i.e. tele-health consultations, digital diagnostics, and remote patient monitoring, are described below. Figure 6 has outlined the smart healthcare system.

#### **4.3.1 Tele-Health Programs**

Tele-health programs apply specifically to hospital appointments that are remote. Tele-health consultations using IoT technology allow doctors to collaborate and support patients remotely in periods of self-isolation, when hospitals are overflowing and healthcare providers are limited. Thanks to tele-health applications, people with debilitating illnesses do not have to access healthcare organizations during the coronavirus outbreak, risking their and others lives, since the required doctor consultation can be performed just by a video call. In such scenario, the patient gets connected using a device having IoT sensors, with remote monitoring of patient's health condition and sends the information obtained to the doctor at the other side. For example, a tele-medicine software created by Softengi allowed any doctor to be reached anywhere. For emergency care, the app is a kind of Uber. In essence, it is a medical expert database that uses various filters to allow the patient to locate the appropriate specialist quickly and to obtain a consultation via a simple smartphone application [62].



Fig. 6 Smart healthcare system

### 4.3.2 Digital Diagnostics

Digital diagnostics is another tele-health facility. Embedded IoT systems are wearable devices offering a self-monitoring tool for their users. The idea is that in a wearable device, myriad IoT sensors easily estimate the health parameters of the patient, promptly providing users with information about their general health status. In times of coronavirus, such usage of IoT devices helped in quick detection and disease treatment, where healthcare workers and patients, both got benefited immensely. For instance, the Kinsa Health Tech Company has developed intelligent thermometers that aggregate data on consumer temperature and symptoms. This real-time data enables Kinsa to track COVID-19 outbreaks in the USA to stream the allocation of health resources [63].

### 4.3.3 Remote Tracking

With IoT technology’s ability to virtually connect doctors with their patients, IoT-driven systems can easily track the state of their users and fully automate patient care workflow by capturing and monitoring data from the IoT device and sending the output to healthcare professionals. Healthcare providers can access real-time patient data as frequently as needed with IoT systems in order to get a greater visibility into the clinical status of the patient. For instance, the Shanghai Public Health Clinical Center (SPHCC) applied a temperature sensing system to monitor patients with COVID-19 to reduce the risk of exposure to coronavirus by caregivers [64].

## 5 Conclusion and Future Scope

The chapter has discussed different problems in different sectors of our society raised due to COVID-19 outbreak and attempted to provide a brief outline of possible solutions for them applying Internet of Things. In view of the outcomes, it can be concluded that to attain the sustainable development goals, some primary policy changes will be entailed through technology and science converged with the digitization, technical advancement and sustainable development fields. The current review chapter tried learning the nature of IoT growth in different application areas during the pandemic simultaneously reaching the sustainable development goals. The focus of IoT in the sustainability factor has been described in the systemic and comprehensive study. The pandemic had a short, mid and long-term effect on numerous society and industry aspects. In the field of digital transformation and sustainability, it was an early attempt to achieve a brainstorming decision in the philosophical context of the COVID-19 report. It also promotes more analysis and dialogue on the bright nexus of SDGs and the digitization process between science and politics.

## References

1. M. Ibrahim, The Fourth Industrial Revolution Combatting COVID-19: The Role of Smart and Sustainable Cities (2020)
2. J.D. Sachs, From millennium development goals to sustainable development goals. *The Lancet* **379**(9832), 2206–2211 (2012)
3. United Nations [UN], Transforming our World: The 2030 Agenda for Sustainable Development (2015). Available at: <https://sustainabledevelopment.un.org/post2015/transformingourworld/publication>. Accessed 14 Feb 2019
4. C.F. Chen, G.Z. de Rubens, X. Xu, J. Li, Coronavirus comes home? Energy use, home energy management, and the social-psychological factors of COVID-19. *Energy Res. Soc. Sci.* **68**(1–5), 101688 (2020)
5. I. Dincer, Covid-19 coronavirus: closing carbon age, but opening hydrogen age. *Int. J. Energy Res.* **44**(8), 6093–6097 (2020)
6. C. Panigutti, A. Perotti, D. Pedreschi, Doctor XAI: an ontology-based approach to blackbox sequential data classification explanations, in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020), pp. 629–639
7. J. Budd, B.S. Miller, E.M. Manning, V. Lampos, M. Zhuang, M. Edelstein, ... M.J. Short, Digital technologies in the public-health response to COVID-19. *Nature Med.* **26**, 1183–1192 (2020)
8. M. Nasajpour, S. Pouriyeh, R.M. Parizi, M. Dorodchi, M. Valero, H.R. Arabnia, Internet of Things for Current COVID-19 and Future Pandemics: An Exploratory Study (2020). arXiv preprint arXiv:2007.11147
9. M.S. Rahman, N.C. Peeri, N. Shrestha, R. Zaki, U. Haque, S.H. Ab Hamid, Defending against the novel coronavirus (COVID-19) outbreak: how can the Internet of Things (IoT) help to save the World? *Health Policy Technol.* **9**(2), 136–138 (2020)
10. A. López-Vargas, M. Fuentes, M. Vivar, Challenges and opportunities of the internet of things for global development to achieve the United Nations sustainable development goals. *IEEE Access* **8**, 37202–37213 (2020)

11. T. Ono, K. Iida, S. Yamazaki, Achieving sustainable development goals (SDGs) through ICT services. *Fujitsu Sci. Tech. J.* **53**(6), 17–22 (2017)
12. T. Osburg, C. Lohrmann, *Sustainability in a Digital World* (Springer, Cham 2017). <https://doi.org/10.1007/978-3-319-54603-2>
13. J. Kähler, F.W. Geels, F. Kern, J. Markard, E. Onsongo, A. Wieczorek, F. Alkemade, F. Avelino, A. Bergek, F. Boons, L. Fünfschilling, An agenda for sustainability transitions research: state of the art and future directions. *Environ. Innov. Soc. Trans.* **31**, 1–32 (2019)
14. C. de Villiers, S. Kuruppu, D. Dissanayake, A (new) role for business—Promoting the United Nations’ Sustainable Development Goals through the internet-of-things and blockchain technology. *J. Bus. Res.* **131**, 598–609, (2020)
15. A. Islam, K. Anum, D. Dwidienawati, S.A. Wahab, A.S.A. Latiff, Building a post COVID-19 configuration between internet of things (IoT) and sustainable development goals (SDGs) for developing countries. *J. Arts Soc. Sci.* **4**(1), 45–58 (2020)
16. C.A. Ionescu, L. Paschia, N.L. Gudanesu Nicolau, S.G. Stanescu, V.M. Neacsu Stancescu, M.D. Coman, M.C. Uzla, Sustainability analysis of the e-learning education system During pandemic period—COVID-19 in Romania. *Sustainability* **12**(21), 9030 (2020)
17. D.G. Roy, B. Mahato, A. Ghosh, D. De, Service aware resource management into cloudlets for data offloading towards IoT. *Microsyst. Technol.* 1–15 (2019)
18. D.G. Roy, B. Mahato, D. De, R. Buyya, Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols. *Future Gener. Comput. Syst.* **89**, 300–316 (2018)
19. D.G. Roy, B. Mahato, D. De, March. A competitive hedonic consumption estimation for IoT service distribution, in *2019 URSI Asia-Pacific Radio Science Conference (AP-RASC)* (IEEE, 2019), pp. 1–4
20. D.G. Roy, P. Das, D. De, R. Buyya, QoS-aware secure transaction framework for internet of things using blockchain mechanism. *J. Netw. Comput. Appl.* **144**, 59–78 (2019)
21. S.E. Bibri, The IoT for smart sustainable cities of the future: an analytical framework for sensor-based big data applications for environmental sustainability. *Sustain. Cities Soc.* **38**, 230–253 (2018)
22. L.L. Idowu, S.H. Park, A new IoT architecture for a sustainable IoT adoption. *Int. J. Comput. Sci. Inf. Technol. Res.* **5**(2), 204–208 (2017)
23. C. Dupont, M. Vecchio, C. Pham, B. Diop, C. Dupont, S. Koffi, An open IoT platform to promote eco-sustainable innovation in Western Africa: real urban and rural testbeds. *Wirel. Commun. Mob. Comput.* **2018** (2018)
24. Z. Qin, F.Y. Li, G.Y. Li, J.A. McCann, Q. Ni, Low-power wide-area networks for sustainable IoT. *IEEE Wirel. Commun.* **26**(3), 140–145 (2019)
25. M. Nitti, V. Pilloni, D. Giusto, V. Popescu, IoT architecture for a sustainable tourism application in a smart city environment. *Mob. Inf. Syst.* **2017** (2017)
26. T. Riedel, N. Fantana, A. Genaid, D. Yordanov, H.R. Schmidtke, M. Beigl, Using web service gateways and code generation for sustainable IoT system development, in *2010 Internet of Things (IOT)* (IEEE, 2010), pp. 1–8
27. D. Mishra, G.C. Alexandropoulos, S. De, Energy sustainable IoT with individual QoS constraints through MISO SWIPT multicasting. *IEEE Internet Things J.* **5**(4), 2856–2867 (2018)
28. S.K. Mishra, D. Puthal, B. Sahoo, S. Sharma, Z. Xue, A.Y. Zomaya, Energy-efficient deployment of edge datacenters for mobile clouds in sustainable IoT. *IEEE Access* **6**, 56587–56597 (2018)
29. V. Gupta, S. Tripathi, S. De, Green sensing and communication: a step towards sustainable IoT systems. *J. Indian Inst. Sci.* **100**(2), 383–398 (2020)
30. S. Alsamhi, O. Ma, M.S. Ansari, Q. Meng, Greening Internet of Things for Smart Everything with a Green-Environment Life: A Survey and Future Prospects (2018). arXiv. arXiv preprint arXiv:1805.00844
31. D. De, A. Mukherjee, A. Ray, D.G. Roy, S. Mukherjee, Architecture of green sensor mobile cloud computing. *IET Wirel. Sens. Syst.* **6**(4), 109–120 (2016)



32. S. Nižetić, P. Šolić, D.L.D.I. González-de, L. Patrono, Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **274**, 122877 (2020)
33. D. Kyriazis, T. Varvarigou, D. White, A. Rossi, J. Cooper, Sustainable smart city IoT applications: heat and electricity management & Eco-conscious cruise control for public transportation, in *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)* (IEEE, 2013), pp. 1–5
34. S. Yim, S. Barrett, Public Health Impacts of Combustion Emissions in the United Kingdom, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge (2012)
35. Z.H. Ali, H.A. Ali, Towards sustainable smart IoT applications architectural elements and design: opportunities, challenges, and open directions. *J. Supercomput.* **77**, 5668–5725 (2021)
36. P.K. Sharma, N. Kumar, J.H. Park, Blockchain technology toward Green IoT: opportunities and challenges. *IEEE Netw.* **34**(4), 263–269 (2020)
37. T. Graziano, Smart technologies, back-to-the-village rhetoric, and tactical urbanism: post-COVID planning scenarios in Italy. *Int. J. E-Plan. Res. (IJEPR)* **10**(2), 80–93 (2021)
38. F. Benkhelifa, H. ElSawy, J.A. Mccann, M.S. Alouini, Recycling cellular energy for self-sustainable IoT networks: a spatiotemporal study. *IEEE Trans. Wirel. Commun.* **19**(4), 2699–2712 (2020)
39. G. del Río Castro, M.C.G. Fernández, Á.U. Colsa, Unleashing the convergence amid digitalization and sustainability towards pursuing the Sustainable Development Goals (SDGs): a holistic review. *J. Clean. Prod.* **280**, 122204 (1–40) (2020)
40. P. Cousin, F. Le Gall, C. Pham, N. Malaguti, P.Y. Danet, S. Ziegler, IoT standards for Africa and sustainable development goals (SDGs), in *2018 IST-Africa Week Conference (IST-Africa)* (IEEE, 2018), p. 1
41. B.M. Nonnecke, M. Bruch, C. Crittenden, *IoT & Sustainability: Practice, Policy and Promise. UC* (Berkeley: Center for Information Technology Research in the Interest of Society (CITRIS), (2016). <https://escholarship.org/uc/item/7dp1t4p8>
42. C.F. Chen, G.Z. de Rubens, X. Xu, J. Li, Coronavirus comes home? Energy use, home energy management, and the social-psychological factors of COVID-19. *Energy Res. Soc. Sci.* **68**(1–5), 101688 (2020)
43. I. Dincer, Covid-19 coronavirus: closing carbon age, but opening hydrogen age. *Int. J. Energy Res.* **44**(8), 6093–6097 (2020)
44. C. Béné, Resilience of local food systems and links to food security—a review of some important concepts in the context of COVID-19 and other shocks. *Food Secur.* **12**, 805–822 (2020)
45. R. Walshe, K. Casey, J. Kernan, D. Fitzpatrick, AI and big data standardization: contributing to United Nations sustainable development goals. *J. ICT Stand.* **8**(2), 77–106 (2020)
46. B. Ekumah, F.A. Armah, D.O. Yawson, R. Quansah, F.E. Nyieku, S.A. Owusu, . . . A.R. Afitiri, Disparate on-site access to water, sanitation, and food storage heighten the risk of COVID-19 spread in Sub-Saharan Africa. *Environ. Res.* **189**, 109936 (1–12) (2020)
47. A. Armin Razmjoo, A. Sumper, A. Davarpanah, Energy sustainability analysis based on SDGs for developing countries. *Energy Sources Part A: Recover. Util. Environ. Effects* **42**(9), 1041–1056 (2020)
48. A.R. Al-Ali, Internet of things role in the renewable energy resources. *Energy Proc.* **100**, 34–38 (2016)
49. V. Kulkarni, R. Mathew, IoT: a step towards sustainability, in *Emerging Trends in Disruptive Technology Management for Sustainable Development* (Chapman and Hall/CRC, 2019), pp. 21–43
50. A. Lakhani, E. Sharma, K. Gupta, S. Kapila, S. Gupta, Corona virus (COVID-19) and its impact on health care workers. *J. Assoc. Physicians India* **68**(9), 66–69 (2020)
51. M. Zarei, A. Rad, Covid-19, challenges and recommendations in agriculture. *J. Bot. Res.* **2** (2020)



52. Containing COVID19 Impacts on Indian Agriculture, <https://www.icrisat.org/containing-covid19-impacts-on-indian-agriculture/>. Last accessed 4 Feb 2021 (2020)
53. P. Carberry, A.K. Padhee, Containing COVID 19 impacts on Indian agriculture. Agri-buzz. ICRISAT-April 18, p. 2020 (2020)
54. B.M. Nonnecke, M. Bruch, C. Crittenden, IoT and sustainability: practice, policy and promise (2016)
55. A. Koehl, Urban transport and COVID-19: challenges and prospects in low-and middle-income countries. *Cities Health* 1–6 (2020)
56. Statista, Number of Vehicles in Use Worldwide 2006–2014. Available online: <https://www.statista.com/statistics/281134/number-of-vehicles-in-use-worldwide/>. Accessed on 12 Feb 2017 (2016)
57. A. Balasubramaniam, A. Paul, W.H. Hong, H. Seo, J.H. Kim, Comparative analysis of intelligent transportation systems for sustainable environment in smart cities. *Sustainability* 9(7), 1120 (2017)
58. F.Y. Wang, S. Tang, Artificial societies for integrated and sustainable development of metropolitan systems. *IEEE Intell. Syst.* 19(4), 82–87 (2004)
59. M. Zarei, A. Mohammadian, R. Ghasemi, Internet of things in industries: a survey for sustainable development. *Int. J. Innov. Sustain. Dev.* 10(4), 419–442 (2016)
60. E.D. Lioutas, C. Charatsari, Enhancing the ability of agriculture to cope with major crises or disasters: what the experience of COVID-19 teaches us. *Agric. Syst.* 187, 103023 (2021)
61. R. Sharma, A. Shishodia, S. Kamble, A. Gunasekaran, A. Belhadi, Agriculture supply chain risks and COVID-19: mitigation strategies and implications for the practitioners. *Int. J. Logist. Res. Appl.* (2020). <https://doi.org/10.1080/13675567.2020.1830049>
62. Telemedicine app, How we developed Uber for Medical Services, <https://softengi.com/projects/telemedicine-app-how-we-developed-uber-for-medical-services/>. Last accessed 4 Feb 2021 (2020)
63. Digital thermometer data may provide insight into COVID-19 surges, <https://www.mobihealthnews.com/news/asia-pacific/sphcc-employs-iot-tech-and-wearable-sensors-monitor-covid-19-patients>. Last accessed 4 Feb 2021 (2020)
64. SPHCC employs IoT tech and wearable sensors to monitor COVID-19 patients, <https://www.mobihealthnews.com/news/asia-pacific/sphcc-employs-iot-tech-and-wearable-sensors-monitor-covid-19-patients>. Last accessed 4 Feb 2021 (2020)

# Reinforced Rider Optimization Algorithm for Diagnosis of Autism Spectrum Disorder and Medical Data



N. B. Arunekumar and K. Suresh Joseph

## 1 Vitals in Brief

Patients who are diagnosed with ASD [1] possess difficulties in having communications and behavioral and social challenges with others. ASD is a disorder that can last all along the life and it can be recognized at any age. But symptoms of ASD can be spotted early in the childhood itself starting at age of 2. ASD isn't race specific and it prevails generically around the globe. Other common traits which ASD-diagnosed patients have are repetitive behaviors and difficulties in functioning at educational institutions. Early diagnosis and treatment would help patients of ASD to increase their ability of functioning [2]. ASD is termed as a spectrum as not all the children show similar behavioral disorders; instead they possess several combinations of them. Severity of the disorder can be clearly visible from CDC survey of parents' report. The report from 2012 has recorded that 1 in 50 children has been affected with ASD and their ages range from 6 to 17 [3]. There are special classes of ASD patients called high-functioning autism spectrum disorder patients who can do better in linguistics of literary works but not well in social context of language [4]. For such children, handwriting is being distinguished [5] from others, and this phenomenon is used as a predictor for diagnosis [6]. It is vital to diagnose the ASD children early and provide them with necessary assistance they need. There are different modalities in identifying ASD patients of which the easiest method to be considered is screening them with questionnaire. There is a specific set of questions which has to be answered by the children based on which those children are being categorized. These screening tests are best to be done after the age of 2 by a professional [7].

---

N. B. Arunekumar (✉) · K. S. Joseph  
Department of Computer Science, Pondicherry University, Puducherry, India

## ***1.1 Imaging the Neuronal Activity***

Preliminary methods to understand the functioning of the brain in pre-era of medical imaging were to examine the brain of people who had abnormalities like infections, injury, and stroke. Such brains with abnormalities will be compared with the ones that are normal, and functionality of the brain over its anatomy was deduced. By this method only abstract functionality was known rather than the event-based functionality. Later, imaging technologies like positron emission tomography (PET) came into usage. These PET imaging had drawbacks such as radiation exposure where a little quantum of radioactive tracers was utilized and excessive time was consumed for imaging. Due to this drawback, PET could not be used on children unless and otherwise it was necessarily needed and the device itself was very sparsely available.

Magnetic resonance imaging (MRI) is one among the noninvasive tools which aids to study the brain as a whole. In general MRI captures anatomical structure of the brain in high resolution as a 3D image recording using the hydrogen nuclei present in water molecules seen in the brain. Special case of MRI is fMRI which is termed as functional MRI. In contradiction to PET, fMRI is safe and could be used for imaging the brain irrespective of age factor. The fMRI modality also works at greater speeds than PET, thus increasing temporal resolution. This higher temporal resolution paved the path for event-related design to capture small stimulus that occurs in our brain. When any mental action is carried out by the brain, the corresponding cells of the brain use oxygen for that activity. In order to regain that oxygen, blood flow is elevated to those respective parts of the brain where the activity took place. Thus, a spike of blood flow could be found in places where the neuronal activity took place. The fMRI detects those changes in oxygenation level using the blood-oxygen-level-dependent (BOLD) signals.

By observing oxygen level in the blood, fMRI could record metabolic structure of the brain over a time span which results as a spatiotemporal data. Analysis of the fMRI data is challenging owing to several other factors which persist on recording the image. Some factors are human-created disturbance such as the head movement, variance that is present among population, and the variance in the thought process, i.e., temporal domain across the people for doing the same event. Factors such as dimension also play a vital role for generalization of an event. Several other important preprocessing steps that have to be carried out on the image are spatial smoothing and normalization where smoothing is to blur off the unnecessary noise present in the image and normalization is to adapt the alignment of data belonging to various individuals over a common framework such that group analysis over the brain signals can be calculated. Motion correction, distortion correction, and slice time correction nullify the errors due to the head movements, spatial distortion, and change in time over different slices, respectively. Temporal frequency filtering averts the noise that may be present on low frequency. After using the combination of all these preprocessing, the 4D time series data of the brain which is ready for classification can be obtained.

The rs-fMRI (resting state FMRI) is a special case of the fMRI which is used to measure the connectivity of the brain. This rs-fMRI is capable of exposing circuits with correlation and anticorrelation on performing specific tasks. These circuits give us a clean picture of effective connectivity that persists over neuronal activity. The rs-fMRI data uses voxels whose correlation is calculated to define connectivity on any action of the brain that results in a high-dimension data. Each voxel is indexed by a 3D coordinate system  $[x\_vox, y\_vox, z\_vox]$  that has values which represents the signal level at respective coordinate positions. The coordinate system of image along each axis with its minimum and maximum is termed as left to right for x-axis, posterior to anterior for y-axis, and superior to inferior for z-axis. Three different viewing angles on 2D pertaining to the 3D coordinates are given by coronal, axial, and sagittal. The coronal view spans across x- and z-axis, axial view spans across x- and y-axis and sagittal view spans across y- and z-axis.

## 1.2 Note on Search Techniques

To select or search optimal solution from several other huge sets of possible solutions, optimization algorithms are being utilized. In general the optimization problem could be modeled as either maximization or minimization problem where optimal solution with minimal value or the maximum value must be found over the search space, respectively. The optimization problem is modeled based on the two important functions which are variable functions and constraint functions. Weights of the variables are being adjusted to find optimal solution from the entire search area. The complete set of possible solutions when adjusting the weights of each variable within the limit of given constraints can be termed as feasible region. The best solution from this feasible region is termed as optimal solution. Optimization problem can be mathematically constituted as in Eq. 1 and Eq. 2:

$$\text{Minimize}(x) \quad f(x) \tag{1}$$

$$\text{Subject to } g_i(x) \leq 0, i = 1, \dots, m \tag{2}$$

$$h_j(x) = 0, j = 1, \dots, p$$

The objective function  $f(x)$  in Eq. 1 is constituted as a minimization problem, and inverse of a minimization problem is termed as maximization problem. The constraints in Eq. 2 can be defined as both inequalities  $g_i(x)$  and equalities  $h_j(x)$ , where  $i$  and  $j$  are the number of constraints, respectively. A problem can have one or more objectives combined together. Likewise there can also be zero or more constraints for the given objective function. Objective function with more than one

objective can be termed as multi-objective optimization, and more than three can be termed as many-objective optimization problem.

The optimization problem can be further classified into linear and nonlinear optimization problem whose search spaces are linear and nonlinear, respectively. The mathematical programming models are very efficient in finding the optimal solution over continuous and low-dimension problems. As the dimensions increase, finding optimal solution would consume a large amount of time for such models.

In contradiction the nature-inspired algorithms can be used for both discontinuous and huge dimensions. Nature-inspired algorithms can be broadly classified into heuristic and meta-heuristic algorithms where heuristic algorithms are problem dependent and meta-heuristic algorithms can be termed as problem independent which assume the problem to be a black box.

The optimization problem is broadly divided into two types based on the search space domain which are convex and non-convex. The convex classes of problems have a set of points from a domain such that all the points formed by linear combination between any two points contained in the domain set must also be present in that domain set itself. If all the points formed as a result of the linear combination are not found in the domain itself, then the domain is defined as non-convex domain. Convex domain has single optimal solution which is minimum for convex functions and maximum for concave functions. Non-convex domain may have multiple discontinuous feasible regions possessing more possible local optimum solutions. Local optimum solution is defined as the best solution among the local cluster of search space. Global optimum solution is considered as the best optimal solution among the complete continuous and discontinuous search spaces. Convex domain would have only one global optima and the search space would be continuous. Non-convex domain problems may have discontinuous search space and therefore have potential local optima with respect to the clusters of points. Convex optimization problem can thus be easily solved using gradient-based methods which follow the slope of the surface to find minimum or maximum. The non-discontinuity and single global optima make it easier to find solution for such class of problems. Non-convex optimization problem owing to discontinuity and complex surface could not be solved by gradient-based methods, and most gradient-based methods would suffer from tangling into local optima instead of global optima.

### ***1.3 Brief on Feature Selection***

Curse of dimensionality [8] affects the generalization capability of data due to unnecessary features. Three major feature selection methodologies that are used for averting such unnecessary features are filter, wrapper, and embedded methods. The filter methods [9] like mutual information [10] and Laplacian score [11, 12, 13] are completely independent of the performance of the classifier which lacks to behave with respect to the classifier's ability over the data. Wrapper method

[14] consumes a considerable amount of time as this method adapts based on the feedback of classifier over the structure of the data. Embedded method [15] measures usefulness of features guided by the learning algorithms and ranks the features. Wrapper method is well suited for measuring feature interactions which is lacking in other two methods. Having  $N$  number of features, there are about  $2^N$  combinations from which the feature selection methods can select features.

Contributions of this chapter are:

- Designing novel RROA a meta-heuristic algorithm based on ROA for wrapper feature selection
- Deploying the proposed RROA algorithm for wrapper feature selection using KNN classification algorithm over medical datasets
- Comparing the proposed RROA wrapper model with other existing meta-heuristic algorithm wrapper models over standard medical datasets to showcase its ability of supremacy
- Designing a diagnosis system using the proposed RROA and wrapper method for classification of ASD using rs-fMRI data with KNN and comparing the RROA with other existing meta-heuristic algorithms over the wrapper model feature selection to prove the efficiency of the proposed algorithm
- Designing a novel semi-wrapper model using the RROA wrapper with max voting ensemble classification algorithm for diagnosis of the ASD using the rs-fMRI

## 2 Summary on the Previous Research

The generic method which is used for diagnosis of ASD is the questionnaire [16, 17], but only by questionnaire that perfect prediction is hard to be found. Another investigation with respect to parents possessing ASD and the possibility of disease being hereditary was being investigated [18, 19]. All these methods of aiding to diagnose ASD are not stable due to several biases. Thus, methods of utilizing the data of the brain were put into effort. The major brain imaging modalities are EEG [20], PET [21], MRI [22], and fMRI [23].

The EEG uses electrodes placed all over the head from which signals are being recorded. EEG with squashing time algorithm has been used to diagnose autism [24], but they have utilized only a small amount of data, where only 15 subjects were put under examination. By using such a mere number of data, generalization is hard. Using molecular imaging via SPECT and PET, experimentation has been carried out for decades. All these earlier studies have been primly carried out over the cerebral blood flow and the glucose metabolism. Most of these studies have only considered a mere number of subjects where the maximum subjects considered are about 150 that use 5-HT synthesis neurotransmitter as the target to investigate the ASD [25]. The neural connectivity was used to diagnose autism in [26] where authors used KNN for clustering input and SVM with tenfold cross validation for diagnosing the

disease. They have acquired an accuracy of about 95.9% with about 19 features. The main drawback encountered in the work was the number of subjects considered, i.e., only 15 were subjected to test.

## ***2.1 Machine Learning in ABIDE***

ABIDE dataset has the data of 1112 individuals where 539 are with ASD and 573 are under typical control, thus representing a near-equal number of sample for each class. The authors [27] extracted pairwise functional connectivity matrix and used them for classification of disease. This work comprised multiple sites from the ABIDE dataset. A total of about 964 subjects were used and about 7266 regions of interests were considered, and linear model was used for the classification. On considering data from sites independently, the authors could achieve accuracy till 90% for certain sites. When considering multisite data, diversity amid the characteristics of data has been increased, and an accuracy of about 60% was being acquired for multisite data. Graph convolution neural networks [28] are a form of artificial neural network that are used to classify graphical data. In [29] the authors have embedded the image features and phenotypic data of subjects to a sparse graph. The sparse graphs have image feature vectors on nodes and phenotypic data on the edges. After embedding they have done a semi-supervised classification using graph convolution neural networks. The authors have devised the classification algorithm and tested for the ASD and Alzheimer's diseases of which 70.4% accuracy have been achieved for the ASD.

The autoencoder is a neural model used for the dimensionality reduction. It encodes the given input feature dimension to a lower-dimension vector. In [30] they have utilized the autoencoders for the dimensionality reduction. The denoising autoencoders [31] threshold the deep layers into a latent vector and try to recreate to original data. The input which was reduced to 100 dimension latent vector was being fed into deep neural network and subjected to classification. The authors could achieve a classification accuracy of about 70% on using the deep learning models [32]. In this work the authors have used autoencoders which encode high-dimension to low-dimension representation of the input. But, the impact of original input feature is lost in such subspace learning algorithms.

## ***2.2 Nature-Inspired Algorithms***

Nature-inspired algorithms are one set of algorithms which are capable of searching the non-convex domains. The nature-inspired algorithms are fabricated from the dynamics which are observed in the nature. The nature-inspired meta-heuristic algorithms are better in searching complex search spaces. The feature selection can be modeled as search problem where an optimal solution with high accuracy and

least number of features is to be searched. Physics-based algorithms, evolutionary algorithms, and swarm intelligence [33] algorithms are some of the subclasses of nature-inspired algorithms.

### 2.2.1 Single-Objective Optimization

#### Physics-Based Algorithms

The physics-based algorithms are developed based on physical phenomenon which can be seen in nature such as simulated annealing [34] which is the process to bring down defects in a material by elevating its heat to high temperature and letting it to decrement temperature slowly. High temperature at initial rate of cooling down depicts random search, whereas low temperature at the final phase of cooling depicts pure greedy descent. Initial random search helps to avert algorithm getting stuck in local optima later on which slow cooling helps to fine-tune the algorithm toward optimal solution. Other important physics-based algorithm is gravitational search algorithm (GSA). The gravitational search algorithm [35] is based on the phenomenon of gravity that acts upon each other over elements in the galactic space like stars and planets. The solutions which are initialized move toward stars based on their gravity. This motion is controlled by three parameters of mass which are passive, inertia, and active masses. After the proposal of initial algorithm, several modifications have been encountered to improve searching capacity of algorithm out of which notable modifications are introduction of the physical entities like black holes, escape velocity, dynamic search methods, behavior of chaos, and crossover operator of genetic algorithm [36].

#### Evolutionary Algorithms

The evolutionary algorithm such as genetic algorithm [37] evolves the given population using evolutionary mechanism found in genes of living species such as selection crossover and mutation. Based on the fitness of whole population, evolution is being done and the final best optimal solution is arrived. The other promising evolutionary algorithm is differential evolution which works based on three operators that are mutation, recombination, and selection. In differential evolution [38] algorithm mutation operator mutates the solution with the help of three other solutions that are chosen at random. Recombination is carried out using donor vector and target vector, while the final selection process is to compare the target vector over trial vector and pick the one which is the best.



## Swarm Intelligence-Based Algorithms

Swarm intelligence algorithms work on the basis of swarming behavior possessed by several animals. These algorithms are mostly inspired by the behavioral pattern using which swarm of animals tackles a problem. Most of these SI algorithms work under two phases which are exploration phase and exploitation phase. In exploration phase the particles search for the potential area where solutions could be found. Once potential area is being identified, refined search process is executed on exploitation phase. The algorithms use these two faces interchangeably in any order to narrow down toward optimal solution. Both these phases must be managed with necessary opportunity or else deficiency in exploration phase may lead the swarm to get stuck with local optima and deficiency in exploitation phase may not lead the swarm to narrow down toward the potential optimal solution. Particle swarm optimization is one among the primly studied and utilized algorithms for several scientific and engineering problems. Particle swarm optimization [39, 40] guides the population based on the best position found so far by complete swarm and the best position which the solution itself has encountered. Gray wolf optimization (GWO) [41, 42] algorithm works based on the hunting behavior of the gray wolf. Hierarchy in pack of wolves which are the alpha, beta, and delta along with shrinking encircling technique to hunt the prey is inspired by GWO algorithm. Hierarchy is depicted in the algorithm such that the three best solutions guide the population to reach optimal solution. Some of the variants of GWO are introduction of levy flight mechanism which is a scale-free walk, chaotic maps [43], and binary variants for the feature selection problems. The whale optimization algorithm [44] works on the basis of hunting behavior of humpback whales. This algorithm uses direct approach to move toward the potential area and uses their bubble net feeding method to trap and capture prey. The shrinking encircling method for approaching prey and spiral mechanism for mimicking the bubble net feeding method are used in the algorithm. Bat algorithm [45, 46] uses the echolocation behavior of bat to hunt [47]. The bat algorithm also uses auto zooming technique to catch the prey. Spider monkey algorithm proposed in the year 2014 is based on the communication and behavioral traits followed by spider monkey for foraging their food. Spider monkeys [48] who live in large group called the parent group utilize fission and fusion mechanism for searching food. Parent group members split up and search for food at different directions which is fission mechanism, and once over they all come together to share the acquired food which is depicted in fusion mechanism. Salp swarm algorithm [49] depicts the chaining behavior of sea salps for their motion. Sea salps are tiny translucent creatures found in deep sea; motion in chain of each salp is based on its predecessor in the chain [50, 51]. Speed and direction of motion for each salp at each dimension toward its predecessors are given by the hyperparameters. Several other algorithms that have been used for the wrapper method are ant lion algorithm [52, 53] and cuckoo search algorithm [54] that uses breeding strategy of cuckoo bird [55]. The biogeography-based algorithm is fabricated based on the phenomenon how living species are spread across.

For ant lion optimizer [52, 53] and binary butterfly algorithm [56], apart from their naive models, enhanced models with chaotic [57] and evolutionary behaviors [58] are also proposed. The abovementioned base algorithms are further enhanced with hybridization of fusing multiple base algorithm features to increase searching performance for various applications.

### 2.2.2 Discrete Optimization

In order to convert the optimization algorithms that work in continuous space to discrete space, transfer functions were introduced [59]. Two families of transfer functions which are the S-shaped and V-shaped transfer functions were introduced for this conversion. The S-shaped functions are variants of sigmoid function. These transfer functions squish the results between values of range 0–1. Binary salp swarm algorithm uses both transfer functions and crossover operators for the feature selection process. For transfer function method, a total of eight transfer functions of which the first four S-shaped transfer functions and the next four V-shaped transfer functions were used, and in the crossover method, the best agent was subjected to crossover operator such that the exploration mechanism of the algorithm is enhanced. The best transfer function variant is compared with several other existing algorithms over various datasets and has proved to be a promising algorithm.

### 2.2.3 Multi-Objective Optimization

All algorithms discussed above could be applied for single-objective optimization. To find an optimal solution that gives a better trade-off for two or more objectives, multi-objective optimization algorithms such as NSGA and multi-objective GWO are being used. Using these algorithms, Pareto front which holds the set of non-dominating solutions can be mined. Various methodologies in solving a multi-objective optimization problem are to simultaneously solve the objectives using multi-objective optimization algorithms, to solve one objective at a time by which the entire set of objectives are solved one by one, and to solve by assigning manual weight for each of the objectives to find the best solution.

All these algorithms mimic the nature's behavior in contrast to them; ROA [60] is an algorithm that is based on a phenomenon where four groups of imaginary riders compete among each other. In ROA there is a strict hierarchy among the group of riders which forbids one rider to enjoy the technique of other rider. Likewise, the usage of local optimum value has proven to be one among the tools to enhance search space in algorithms like PSO. Thus, to overcome deficiency in acquiring variability of behavior and utilizing benefit of local optimum solutions, RROA algorithm has been proposed based on ROA algorithm.

### 3 Preliminaries

#### 3.1 Feature Selection

The wrapper feature selection being a multi-objective optimization problem has two criteria of choosing the least subset of features and providing the highest accuracy which can be constituted using the following Eq. 3:

$$Fit = \eta * \psi_R(F) + \omega * \frac{|K|}{|N|} \tag{3}$$

In Eq. 3, the first part  $\psi_R(F)$  represents error rate given by (error rate = 1-accuracy), and the second part represents the number of features where  $|K|$  gives the number of features selected and  $|N|$  is the total number of features. The number of features is presented by a feature vector mask where 1 represents to select a feature and zero to discard it as given in Fig. 1.

The constants  $\eta$  and  $\omega$  depict the importance of those objectives in fitness function, while  $\eta$  is given by  $\eta = 1 - \omega$ .

#### 3.2 Dataset and Preprocessing

The publicly available ABIDE dataset has a 4D fMRI images which are of rs-fMRI type. The data has the rs-fMRI images of 1112 subjects of various age groups ranging from 2 to 70. The children from age of 2–18 are 485 in nos., 2–11 are 308 in nos., 19–29 are 228 in nos., 30–39 are 68 in nos., 40–49 are 17 in nos., 50–59 are 5 in nos., and 60–69 is 1 in no. (Fig. 2)

To acquire the time series data, C-PAC pipeline of preprocessing is done over fMRI images. Pipeline includes masking and registering the atlas and then extracting time series for different regions of the brain. With time series being extracted, the connectivity matrix is constructed using partial correlation between time series signals as shown in Fig. 3. Using the `abide.rois_cc200` derivative, connectivity matrix is being calculated. Along with the connectivity matrix which is flattened, the phenotypic data is being embedded to form a complete feature vector. The data comprises a total of about 19,907 features with 2 classes of ASD and normal patients. The dataset is split into an 80–20 ratio for training and testing.

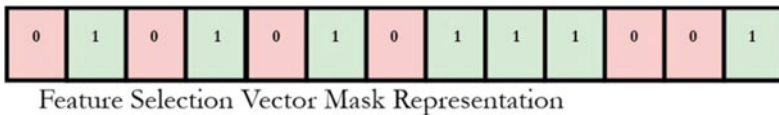


Fig. 1 Feature selection vector

Fig. 2 fMRI representation

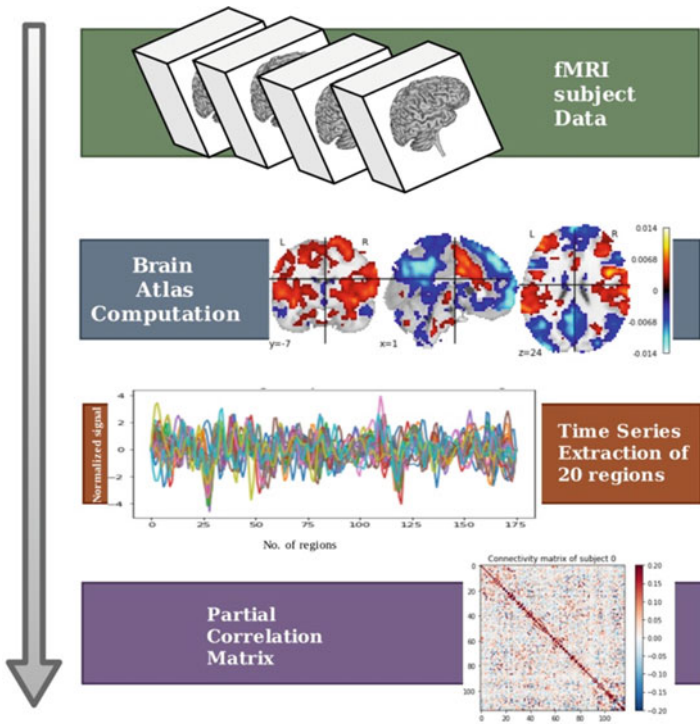
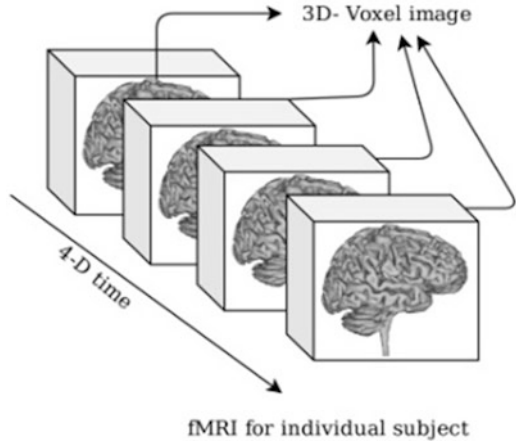


Fig. 3 ASD classification preprocessing pipeline

### 3.3 Rider Optimization Algorithm

The rider optimization algorithm is one among its kind which is based on an imaginary scenario where a group of riders compete with each other. The riders are segregated as four groups who follow different characters designated as per the group they pertain. Each group follows separate strategy but all the rider's motive is to find the target. Most of the early bioinspired algorithms possess meta-heuristics that are common for all the solutions, but the diversity introduced among the population is a special concern for this optimization algorithm. The four groups of riders are the bypass rider, follower, overtaker, and attacker who are abbreviated by B, O, F and A, respectively. The physical devices that are used to control a vehicle are also encoded as steering given by steering angle brake, accelerator, and gear which are encoded as the hyperparameters T, b, e, and K, respectively.

#### 3.3.1 Parameter Initialization

The total numbers of riders are given as N who are divided into four groups as given in Eqs. 4 and 5:

$$N = B + F + O + A \quad (4)$$

$$B = F = O = A = N/4. \quad (5)$$

Variable  $X^t$  is the position of rider at the time t and D is the total number of dimensions of the problem. At initial stage where  $t = 0$ , all the riders are initialized with random values between the bound of each dimension, only after the first round, from  $t = 1$  the riders are updated as per their group to which belong to:

$$X^t = \{ X^t(i, j) \}; 1 \leq i \leq N; 1 \leq j \leq D \quad (6)$$

The control hyperparameters are initialized as in Eq. 7 to Eq. 9:

$$b = \{b_i\}; 1 \leq i \leq N \quad (7)$$

$$K = \{K_i\}; 1 \leq i \leq N \quad (8)$$

$$e = \{e_i\}; 1 \leq i \leq N \quad (9)$$

$$T^t = \{T_{i,j}^t\}; 1 \leq i \leq N; 1 \leq j \leq D \quad (10)$$

The other vital parameter is the top speed of the rider  $V_{max}^i$  given by Eq. 11 where the numerator depicts the difference between the upper and lower bound of the rider position and the denominator  $T_{OT}$  defines off time. The success rate is deduced by the difference between target  $L_T$  and current position  $X_i$  where the rider resides as depicted in Eq. 12. Based on the top speed, the speed limit  $V_i^!$  is being calculated:

$$V_{max}^i = \frac{X_U^i - X_L^i}{T_{OT}} \tag{11}$$

$$sr_i = \frac{1}{\|X_i - L_T\|} \tag{12}$$

Leader of the population is calculated based on fitness or the success rate. The leader solution is updated after completion of an iteration using the solution with best success rate in that respective iteration.

### 3.3.2 Bypass Rider

The bypass rider is the most stochastic rider whose update equation relies on more number of random parameters. The parameters  $\delta$  and  $\beta$  are hyperparameters which may be a random number amid range 0 and 1. The parameters  $\eta$  and  $\xi$  choose a random value amid range 1 and R in overall update equation as given by Eq. 13:

$$X_{t+1}^B(i, j) = \delta [X_t(\eta, j) * \beta(j) + X_t(\xi, j) * [1 - \beta(j)]] \tag{13}$$

### 3.3.3 Follower Rider

The follower as termed updates equation relying on leader who is already selected as given in Eq. 14:

$$X_{t+1}^F(i, k) = X^L(L, k) + \left[ \cos(T_{i,k}^t) * X^L(L, k) * dis_i^t \right] \tag{14}$$

The L in  $X^L$  defines leader index, k defines dimension, the remaining distance which has to be traveled is given by  $dis_i^t$  as in Eq. 15, and  $T_{i,k}^t$  defines the steering angle of rider i:

$$dis_i^t = vel_i^t * (1/T_{OT}) \tag{15}$$

The parameter  $vel_i^t$  defines velocity given by Eq. 16 where  $V_{max}^i$  defines top speed and k in Eq. 14 is based on the coordinate selector as given on Eq. 17 where t is the current time, and on-time probability is given by  $P_{ON}^t$  (Fig. 4):

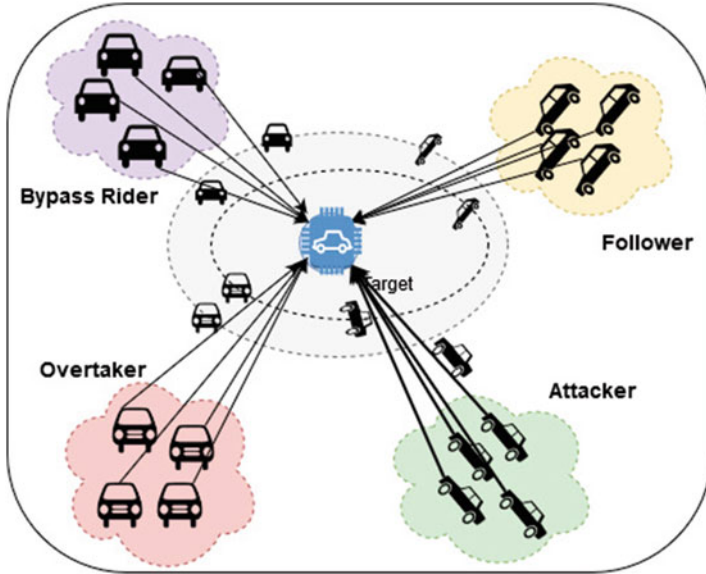


Fig. 4 Riders of ROA

$$vel_i^t = \frac{1}{3} [E_i^t * V_i^l + V_{max}^i * c_i^t + (1 - K_i^t) * V_{max}^i] \tag{16}$$

$$P_{ON}^t = (t/T_{OT}) * Q \tag{17}$$

### 3.3.4 Overtaker Rider

The overtake update using Eq. 18 also uses coordinate selector and  $D_t^I(i)$  the direction indicator. Direction indicator is based on relative success rate  $S_t^R(i)$  which is the probability of success rate given by Eq. 19 (Table 1):

$$X_{t+1}^O(i, k) = X_t(i, k) + [D_t^I(i) * X^L(L, k)] \tag{18}$$

$$S_t^R(i) = r_t(i) / \max_{i=1}^R r_t(i) \tag{19}$$

**Table 1** Pseudo code for ROA

Rider optimization algorithm	
1	Random rider initialization $X_t$ , $t = 1$ to $N$
2	Initialize the hyperparameters angle of steering $T$ , brake $K$ , accelerator $e$ , and gear $E$
3	$r_t$ – success rate is calculated
4	While iterations < maximum iterations
5	for $i = 1$ to $N$
6	Update position of bypass rider using Eq. 9
7	Update position of follower rider using Eq. 10
8	Update positions of overtaker rider using Eq. 15
9	Update positions of attacker rider using Eq. 17
10	Use success rate $r_t$ to rank the riders as in Eq. 16
11	Choose the rider with the highest success rate as leader
12	Update the hyperparameters $T$ , $b$ , $e$ , and $K$
13	Return the leader $X^l$
14	Iterations = iterations + 1
15	End for
16	End while
17	Terminate

### 3.3.5 Attacker Rider

The attacker position update equation is similar to that of follower equation that updates values using steering wheel angle as given in Eq. 20, and the hyperparameters are updated based on rider's current positions:

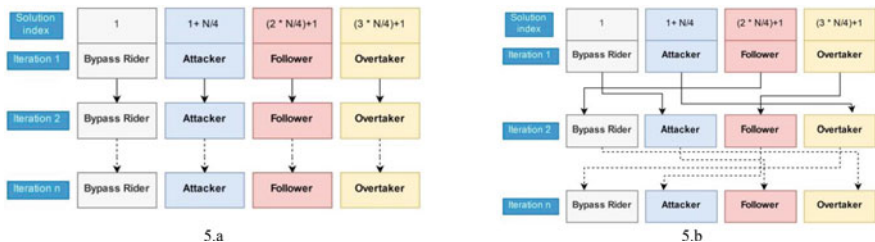
$$X_{t+1}^A(i, j) = X^L(L, j) + \left[ \cos(T_{i,j}^t) * X^L(L, j) \right] \quad (20)$$

## 4 Proposed Algorithm

### 4.1 Proposed Reinforced Rider Optimization Algorithm

The main drawback of rider optimization algorithm is the fixed behavior of each member in rider group. By constraining the behavior, a rider could not adapt other rider's behavior which eliminates interoperability between search techniques. By enabling each rider to stochastically choose modality of search, the iterative behavior of searching by rider is complemented with collaborative behavior. For such a collaboration, dynamic indexing is being used. In original rider optimization algorithm, the riders are split based upon the order in which they are initialized. Each rider with index  $i$  is segregated among  $N/4$  groups based on the index assigned initially, and the same index is utilized to determine their behavior till the end. In





**Fig. 5** (a) Flow of ROA and (b) flow of RROA

dynamic indexing, for each group same  $N/4$  numbers of indices are chosen but are done stochastically. On commencement of iteration, indices of the riders are reinitialized such that a rider can follow any of the four traits in each of the iteration as shown in Fig. 5b. For illustration the first solutions among each of the group are alone taken into consideration as shown in Fig. 5a and b. A better search could be ensured by this strategy both in the initial and the final stages. The personal best solution has been one among the prime influencing factors during the search in algorithms like particle swarm optimization. By introducing the influence of personal best solution as in Eq. 22, algorithm possesses a better chance of finding optimal solution. In Eq. 22,  $rand$  is the random variable between 0 and 1, and  $vel_p$  is the personal velocity derived from Eq. 21 where  $p_b(i)$  is the personal best of the rider  $i$ . Adding both the above features to the existing rider optimization algorithm, the reinforced rider optimization algorithm has been proposed:

$$vel_p = X^t(i) - p_b(i) \quad (21)$$

$$X^{t+1}(i) = X^t(i) + rand * vel_p \quad (22)$$

## 5 Experimentation and Results

The experimentation is carried out using two phases where the first phase is carried out on the generic medical datasets and the second phase is carried out on the challenging ASD dataset for the classification.

### 5.1 Wrapper Feature Selection

The proposed RROA algorithm is used for wrapper feature selection, and KNN algorithm which is nonparametric decides the class of sample based on the nearest

neighbor's sample where  $k$  parameter decides the number of neighbors. The  $k$  neighbors assumed are 5 and Euclidean distance is used for calculating distance between neighbors. For both the ABIDE and medical datasets, training and testing data is being split into ratio of 80% and 20%, respectively. For increasing accuracy of the classifier on real data, K-fold cross validation is being incorporated over the KNN algorithm, and the  $K$  assumed here is 10. The tenfold cross validation error is utilized as the error  $\psi_R(F)$  in Eq. 1. The weight of the  $\eta$  is given as 0.1 and the weight of  $\omega$  is calculated as  $(1 - \eta)$ . All the hyperparameters  $K$  for cross validation,  $k$  for nearest neighbors, and  $\eta$  derived from the literature.

## 5.2 Wrapper Model over Medical Data

In a pre-context to generalize the behavior of proposed RROA algorithm before testing on high-dimensional ASD diagnosis, eight of the generic medical low-dimensional datasets are first subjected to test with wrapper algorithm. All medical datasets are downloaded from standard dataset repositories whose details are being given in Table 2.

For each of the dataset, classification was carried out using tenfold cross validation. For each algorithm, 16 agents were run for 200 iterations on one experiment. Overall 30 independent experimentations were carried out for each dataset, and the accuracies, fitness, and resulting dimensions were recorded. The proposed algorithm was compared with other existing algorithms given in literature over the above-given metrics. The proposed RROA algorithm has selected the best features that can provide a very good overall accuracy than other existing algorithms as visualized in Table 3. It has surpassed other algorithms in nearly 60% of datasets. Even on datasets which it has failed, proposed RROA has bestowed a considerable good accuracy when comparing to the other algorithms. Individually, the proposed RROA algorithm has an outbeaten GWO, BGWO, BGSA, ALO, and SSA algorithms over 75% of datasets. It has also surpassed RROA, BBA, BSSA, and BBO by 87% and BPSO by 100% on tested datasets which can be visually interpreted over Fig. 6.

The fitness comparison of existing algorithm is given in Table 4. The proposed algorithm outperforms other existing algorithms over 75% of datasets. Considering individually, the proposed algorithm surpasses over 87% of data on ROA and BSSA, 75% of data over ALO and BBO and over 60% on GWO, BGWO, BPSO, BBA, and BGSA.

**Table 2** No. of dimensions of the low-dimension medical datasets

Dataset	No. of features	Dataset	No. of features
Bupa	5	Parkinson's	22
Wisconsin	9	Relax	12
Diabetics	8	Heart	9
HCC	49	SPECTF	44

**Table 3** Accuracy comparison over the existing algorithms for low-dimensional medical dataset

	No-FS	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
Bupa	0.680	0.756	0.749	0.748	0.764	0.745	0.754	0.760	0.749	0.760	0.754	<b>0.765</b>
Wisconsin	0.914	0.929	<b>0.933</b>	0.932	0.926	0.928	0.930	0.929	0.925	0.930	0.933	0.913
Diabetics	0.661	0.676	<b>0.691</b>	0.682	0.685	<b>0.691</b>	0.686	0.683	0.679	0.686	0.689	0.687
HCC	0.460	0.625	<b>0.633</b>	0.590	0.612	0.605	0.605	0.582	0.613	0.609	0.593	0.619
Parkinson's	0.902	0.912	0.914	<b>0.930</b>	0.918	0.906	0.906	0.924	0.924	0.906	0.908	0.910
Relax	0.507	0.582	0.597	0.606	0.590	0.597	0.586	0.592	0.596	0.610	<b>0.608</b>	0.544
Heart	0.568	0.614	<b>0.615</b>	0.608	0.596	0.603	0.601	0.601	0.605	0.609	0.614	0.603
SPECTF	0.650	0.707	<b>0.724</b>	0.715	0.694	0.697	0.702	0.705	0.694	0.701	0.697	0.687
<b>Avg Acc.</b>	0.671	0.725	<b>0.732</b>	0.726	0.723	0.722	0.721	0.722	0.723	0.726	0.724	0.716
<b>Rank</b>	12	4	<b>1</b>	2	6	9	10	8	7	3	5	11

As in Table 5, the optimal dimensions have been got by wrapper algorithm using RROA. Even though BBO has identified the least dimensions, it could not achieve the highest accuracy which is due to problem of encountering the local minima. But the RROA algorithm has identified the best features such that the highest accuracy and lowest fitness have been acquired.

In the first phase, the proposed algorithm has been tested over standard repository datasets where the wrapper algorithm has proved to provide the best results when comparing the existing algorithms.

### 5.3 *Semi-Wrapper for ASD Diagnosis*

The wrapper feature selection shows an effective way to compute the dependency between features from above experiments. The features from correlation matrix and phenotypic values are combined to form a vector of  $n$  features. Even with such an efficacy, there is paucity in its performance when the number of dimension increases or the complexity of classifier increases. To aid this situation, the proposed model adopts a semi feature selection algorithm as shown in Fig. 7. The vector is subjected to normalization with respect to each dimension. After normalization, the feature vector is subjected to wrapper feature selection model with KNN classification algorithm. In this wrapper model, the same configurations are set as in the earlier low-dimension feature selection methods. After subjecting to experiment, it was noted that KNN algorithm is failing to perform up to the mark in disease classification. Therefore, to enhance accuracy further, the hybrid wrapper model for an ensemble learning classifier is proposed. The ensemble learning model comprises three different classifiers that learn and vote on the same dataset. In this pipeline naive Bayes classifier, random forest classifier with 250 trees, and SVM classifier with RBF kernel are being used. The vote from each classifier is being bought, and the maximum vote methodology is adopted to classify final result. The naive Bayes classifier algorithm [61] works based on the Bayes theorem with

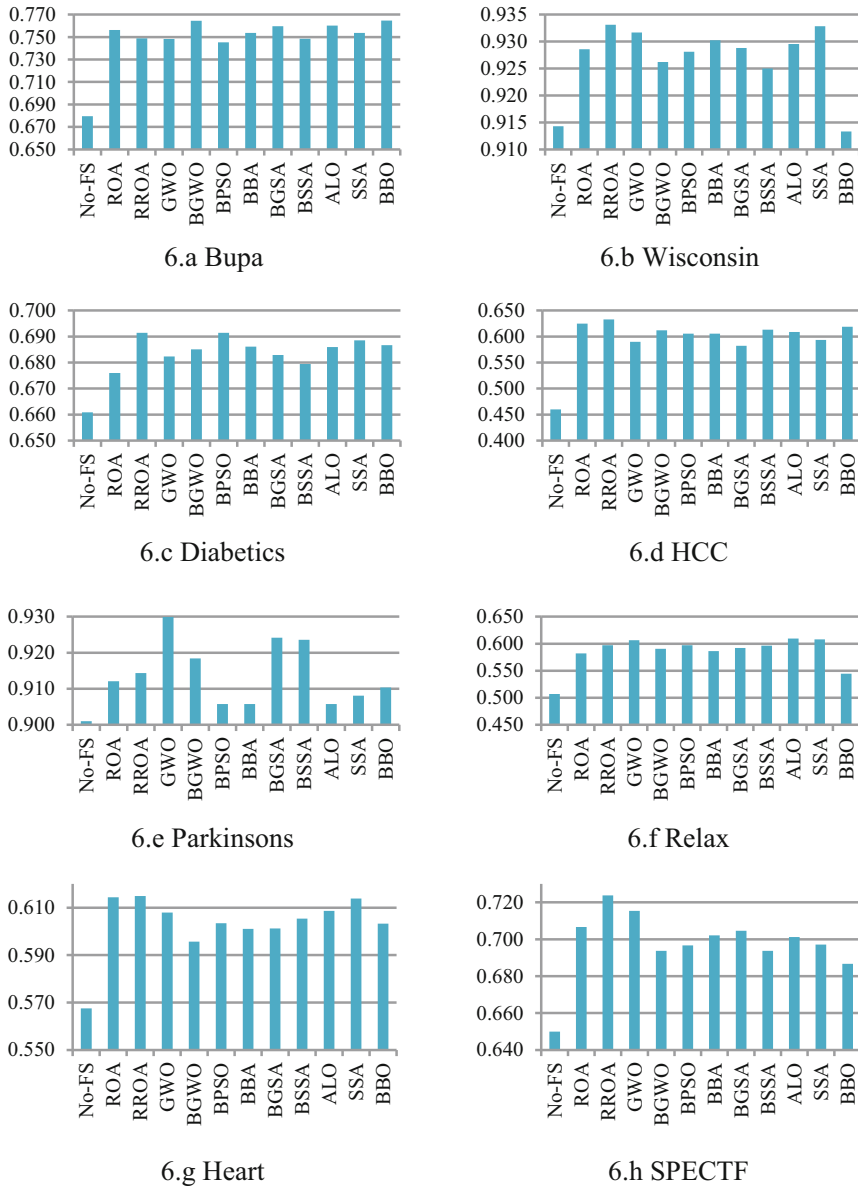


Fig. 6 Comparison of accuracy over medical dataset

the main assumption that there is no conditional dependency between features. High scalability and resistance over curse of dimensionality with less number of training samples are achieved due to the assumption of independence. The naive

**Table 4** Fitness comparison over the existing algorithms for low-dimensional medical dataset

	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
Bupa	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>	<b>0.991</b>
Wisconsin	0.034	<b>0.017</b>	0.018	0.019	0.018	0.019	0.022	0.019	0.019	0.018	0.023
Diabetes	0.235	<b>0.209</b>	0.210	0.212	0.212	0.215	0.219	0.216	0.213	0.212	0.232
HCC	0.266	<b>0.210</b>	0.224	0.218	0.213	0.221	0.211	0.231	0.221	0.216	0.264
Parkinson's	0.156	0.122	0.112	0.120	0.115	0.118	0.112	0.127	0.117	0.114	0.155
Relax	0.296	0.256	0.234	0.256	0.251	0.253	0.233	0.267	0.252	0.245	0.237
Heart	0.288	<b>0.245</b>	0.259	0.281	0.276	0.258	0.263	0.277	0.259	0.251	0.245
SPECTF	0.150	<b>0.095</b>	0.099	0.122	0.119	0.126	0.127	0.137	0.125	0.119	0.162
RANK	13	<b>1</b>	2	8	5	9	6	12	7	3	10

**Table 5** Dimension comparison over the existing algorithm

	No-FS	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
Bupa	<b>5</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>
Wisconsin	9	<b>4</b>	<b>4</b>	5	8	6	6	6	7	7	6	<b>4</b>
Diabetes	8	5	<b>4</b>	5	6	6	5	5	6	6	5	<b>4</b>
HCC	49	17	22	15	34	22	25	24	26	21	22	<b>3</b>
Parkinson's	22	8	4	8	15	10	11	11	12	10	10	<b>3</b>
Relax	12	3	<b>2</b>	3	7	5	4	4	5	3	5	<b>2</b>
Heart	9	<b>2</b>	4	3	6	<b>2</b>	<b>2</b>	3	3	<b>2</b>	<b>2</b>	<b>2</b>
SPECTF	44	14	20	13	30	22	21	22	25	20	20	<b>2</b>
RANK	12	2	4	3	11	5	6	8	10	7	9	<b>1</b>

Bayes algorithm also has high learning speed and is competitive over sophisticated algorithms for its efficiency.

The naive Bayes classifier works by constructing joint probability distribution over which Bayes theorem and prior probabilities of classes are being utilized for a given feature vector  $X$  which has features 1 to  $n$   $X = \{x_1, \dots, x_n\}$  and classes  $Y_m$ . The probability for an unknown sample to be a particular class given as  $Y'$  is calculated by Eq. 23 which follows the chain rule:

$$Y' = \underset{k \in \{1, \dots, K\}}{\text{argmax}} p(C_k) \prod_{i=1}^n p(x_i | C_k) \tag{23}$$

Linearly separable data are the ones which can be bifurcated using a single straight line. As a straight line can only work on two dimensions, the hyperplane is used when data is more than three dimensions. Being derived from equation of straight line  $y = ax + b$ , equation of a hyperplane can be given as  $wx + b$ , where  $w$  is a multi-dimension vector that corresponds to the slope of hyperplane at each dimension. There could be an infinite number of hyperplanes to separate the given classes, but choosing the best one which is amid both the classes would provide better classification results. To maximize such distance where hyperplane

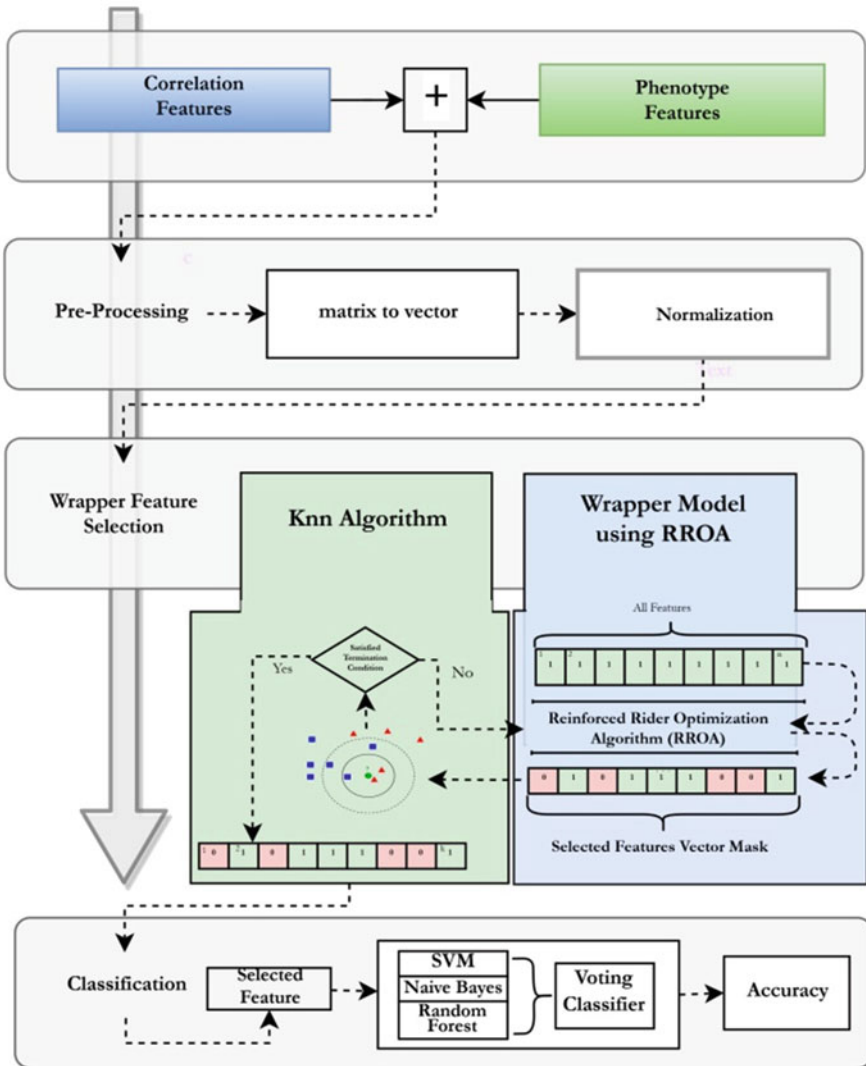


Fig. 7 Pipeline for ASD diagnosis

is equidistant from both the classes, support vectors are being used. The SVM classifier uses hyperplane and the support vectors to differentiate the linearly separable data:

$$y_i (w \cdot x_i) + b - 1 \geq 0 \text{ for } y_i = +1, -1 \tag{24}$$

**Table 6** Accuracy comparison for ASD diagnosis

	No-FS	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
ABIDE	0.492	0.516	<b>0.536</b>	0.503	0.526	0.523	0.507	0.502	0.507	0.529	0.526	0.510
Rank	12	6	<b>1</b>	10	3	5	8	11	8	2	3	7

**Table 7** Fitness comparison for ASD diagnosis

	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
ABIDE	0.4142	<b>0.372</b>	0.3832	0.379	0.3894	0.3812	0.3867	0.3867	0.3853	0.3833	0.3833
Rank	11	<b>1</b>	4	2	10	3	8	8	7	5	5

The SVM classifier [62] works based on the hypothesis as in Eq. 24 where the given unknown sample is subjected to dot product with the hyperplane which is being learned. Based on the result of the dot product, if it is nonnegative, the sample belongs to class B or else to class A. There are several methods for optimizing support vector machine such that hyperplane and the support vectors fit with the maximum margin between the two classes. Optimizing the position of hyperplane and support vectors is a constrained optimization problem which is quadratic. Being quadratic, the problem has a single global minimum and a smooth surface; therefore, gradient-based algorithms would be better to solve for the best optimal position. For linearly inseparable data, the kernel trick [63, 64] is used to convert the data such that it's linearly separable. The RBF – radial basis function – kernel [65] is used for this experiment for the SVM classification.

Decision trees are one of the algorithms whose logic can be interpreted and are near to mimic human-level reasoning. The logic behind each decision is clearly visible when decision trees are being used. Decision tree is built upon tree-like data structure which comprises nodes, branches, and leaves. From the given samples, each feature in vector X is represented by the nodes, and decision rules pertaining to that features are recorded in branches while respective class  $Y_k$  is given in leaves. On training process of decision tree, a whole set of rules are being constructed. There are several algorithms to construct decision tree of which CART and ID3 have been used exhaustively. On training with cart algorithm, Gini index is used as a metric, and while training with ID3, entropy is used as a metric. The random forest [66] classifier is a collection of decision trees [67, 68].

For initial feature selection with KNN, RROA algorithm is used. The accuracies obtained using the wrapper models over the RROA and existing algorithms are compared on Table 6.

It can be depicted from Table 7 that the proposed algorithm performs well than the other existing algorithms whose fitness is compared on the table.

It is evident from Table 8 that the least number of features selected by the RROA algorithm has been the minimal feature set for maximum accuracy for the KNN algorithm. To increase efficiency, the selected features are subjected to the ensemble classification algorithm which finally results in an accuracy of 75%. Features selected by the other algorithms are also subjected to comparison, and

**Table 8** Number of dimensions selected for comparison for ASD diagnosis

	No-FS	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
ABIDE	19,907	2174	<b>1159</b>	7131	13,719	9942	9966	9897	11,348	5353	9953	10,044
Rank	12	2	<b>1</b>	4	11	6	8	5	10	3	7	9

conclusively the features selected by the proposed algorithm have been the best set of features such that it performs well even on the ensemble model as shown in Table 9.

From Fig. 8 it can be clearly visible that RROA has selected features that are well optimized such that irrespective of the classifier being utilized, accuracy for classification is found to be the best. The proposed algorithm has been tested over feature selection models and proved to perform best in terms of fitness and accuracy. Pertaining to time complexity, the additional statements of dynamic index and inclusion of personal best add up to  $O(1)$  inside the main loop of the RROA algorithm. Thus, without any addition to the time complexity of the existing algorithm, the proposed RROA algorithm performs better.

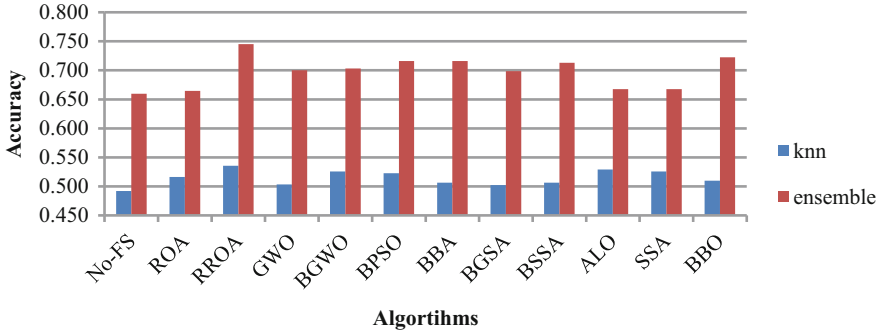
## 6 Conclusion and Future Scope

A novel reinforced rider optimization algorithm has been proposed with two additional characteristics of dynamic indexing and inclusion of personal best. The dynamic indexing improves interoperability between characteristics of solution, and addition of personal best helps the solution to search in more effective area. The proposed algorithm has been tested under two different feature selection experimentations for medical data, where the first experimentation uses datasets of low dimensions and the second experimentation uses the challenging ASD biomarker identification from ABIDE dataset which uses rs-fMRI data. The medical dataset experimentation is conducted only with wrapper feature selection using RROA and KNN algorithm, while ASD diagnosis incorporates semi-wrapper algorithm for improved diagnosis. The proposed RROA algorithm has outperformed on 60% of low-dimension medical datasets over the prime nature-inspired existing algorithms in terms of accuracy and fitness without any additional time complexity than existing algorithm. In case of ASD diagnosis also, the proposed RROA has outbeaten other algorithms with 75% of accuracy. From results and comparison, it can be concluded that proposed RROA algorithm works better with both low-dimensional and high-dimensional datasets. There are other psychiatric disorders like schizophrenia and mental illness that can be diagnosed with the help of fMRI data; in the future the proposed model could be extended to investigate biomarkers for such diseases.



**Table 9** Comparison of accuracy for ASD diagnosis over semi-wrapper model

	No-FS	ROA	RROA	GWO	BGWO	BPSO	BBA	BGSA	BSSA	ALO	SSA	BBO
ABIDE	0.6597	0.6645	<b>0.7482</b>	0.7	0.7032	0.7161	0.7161	0.6987	0.7129	0.6677	0.6677	0.7226
Rank	12	11	<b>1</b>	7	6	3	3	8	5	9	9	2



**Fig. 8** Comparison of accuracy for wrapper and semi-wrapper model for ASD diagnosis

## References

1. N. Marrus, J.N. Constantino, Autism spectrum disorders, in *Reference module in neuroscience and biobehavioral psychology*, (Elsevier, 2019)
2. J. Jennings Dunlap, Autism spectrum disorder screening and early action. *J. Nurse Pract.* **15**(7), 496–501 (Jul. 2019)
3. P. Rane, D. Cochran, S. M. Hodge, C. Haselgrove, D. N. Kennedy, J. A. Frazier, Connectivity in Autism: A Review of MRI Connectivity Studies, in *Harvard Review of Psychiatry*, vol. 23, no. 4. Taylor and Francis Ltd, pp. 223–244 (01-Jan-2015)
4. S. L. J. Jackson, F. R. Volkmar, Diagnosis and Definition of Autism and Other Pervasive Developmental Disorders, in *Autism and Pervasive Developmental Disorders*, Cambridge University Press, (2019), pp. 1–24
5. S. Rosenblum, H.A. Ben Simhon, E. Gal, Unique handwriting performance characteristics of children with high-functioning autism spectrum disorder. *Res. Autism Spectr. Disord.* **23**, 235–244 (Mar. 2016)
6. S. Rosenblum, H. Amit Ben-Simhon, S. Meyer, E. Gal, Predictors of handwriting performance among children with autism spectrum disorder. *Res. Autism Spectr. Disord.* **60**, 16–24 (Apr. 2019)
7. C. Lord, S. Risi, P.S. DiLavore, C. Shulman, A. Thurm, A. Pickles, Autism from 2 to 9 years of age. *Arch. Gen. Psychiatry* **63**(6), 694–701 (Jun. 2006)
8. J. Li et al., Feature selection: A data perspective, Jan. 2016
9. H. Liu, H. Motoda, *Feature selection for knowledge discovery and data mining* (Springer US, 1998)
10. M. Zaffalon, M. Hutter, Robust feature selection by mutual information distributions, in *Proceedings of the Eighteenth Conference on Uncertainty in Artificial Intelligence*, (2002), pp. 577–584
11. X. He, D. Cai, P. Niyogi, Laplacian score for feature selection. *Adv. Neural Inf. Process. Syst.*, 507–514 (2005)
12. S. Güneş, K. Polat, Ş. Yosunkaya, Multi-class f-score feature selection approach to classification of obstructive sleep apnea syndrome. *Expert Syst. Appl.* **37**(2), 998–1004 (Mar. 2010)
13. A. Zafra, M. Pechenizkiy, S. Ventura, ReliefF-MI: An extension of ReliefF to multiple instance learning. *Neurocomputing* **75**(1), 210–218 (Jan. 2012)
14. S. Arora, P. Anand, Binary butterfly optimization approaches for feature selection. *Expert Syst. Appl.* **116**, 147–160 (2018)
15. S. Lee, S. Kim, Marginalized lasso in sparse regression. *J. Korean Stat. Soc.* **48**(3), 396–411 (Sep. 2019)

16. S.K. Berument et al., Autism screening questionnaire: diagnostic validity: pre-linguistic autism diagnostic observation schedule adapted for older individuals with severe to profound mental retardation: a pilot study. *Br J Psychiatry* **175** (1999)
17. P.A. Filipek et al., The screening and diagnosis of autistic spectrum disorders 1. *J Autism Dev Disord* **29**(6), 439–484 (1999)
18. R. Martins, I. Bonito, A. Andrade, C. Albuquerque, C. Chaves, ScienceDirect the impact of the diagnosis of autism in parents of children. *Procedia-Social Behav. Sci.* **171**, 121–125 (2015)
19. A.S. Rabba, C. Dissanayake, J. Barbaro, Parents' experiences of an early autism diagnosis: Insights into their needs. *Res. Autism Spectr. Disord* **66** (Oct. 2019)
20. N. Muramoto, N. Matsui, T. Isokawa, SICE, Searching Ability of Qubit-Inspired Genetic Algorithm. 2012 Proc. Sice Annu. Conf **3**, 443–446 (2012)
21. Z. Cai, S. Li, D. Matuskey, N. Nabulsi, Y. Huang, PET imaging of synaptic density: A new tool for investigation of neuropsychiatric diseases, *Neuroscience Letters*, vol. 691. Elsevier Ireland Ltd, pp. 44–50, 19-Jan-2019
22. U.A. van der Heide, M. Frantzen-Steneker, E. Astreinidou, M.E. Nowee, P.J. van Houdt, MRI basics for radiation oncologists. *Clin. Transl. Radiat. Oncol.* **18**, 74–79 (Sep. 2019)
23. S.H. Hojjati, A. Ebrahimzadeh, A. Khazae, A. Babajani-Feremi, Predicting conversion from MCI to AD by integrating rs-fMRI and structural MRI. *Comput. Biol. Med.* **102**, 30–39 (Nov. 2018)
24. E. Grossi, C. Olivieri, M. Buscema, Diagnosis of autism through EEG processed by advanced computational algorithms: A pilot study. *Comput. Methods Prog. Biomed.* **142**, 73–79 (Apr. 2017)
25. N. R. Zürcher, A. Bhanot, C. J. McDougale, J. M. Hooker, A systematic review of molecular imaging (PET and SPECT) in autism spectrum disorder: Current state and future research opportunities, *Neuroscience and Biobehavioral Reviews*, vol. 52. Elsevier Ltd, pp. 56–73, 01-May-2015
26. G. Deshpande, L.E. Libero, K.R. Sreenivasan, H.D. Deshpande, R.K. Kana, Identification of neural connectivity signatures of autism using machine learning. *Front. Hum. Neurosci.* (7), 670 (Oct. 2013)
27. J.A. Nielsen et al., Multisite functional connectivity MRI classification of autism: ABIDE results. *Front. Hum. Neurosci.* **7**, 599 (2013)
28. A. Qin, Z. Shang, J. Tian, Y. Wang, T. Zhang, Y.Y. Tang, Spectral–spatial graph convolutional networks for semisupervised hyperspectral image classification. *IEEE Geosci. Remote Sens. Lett.* **16**(2), 241–245 (Feb. 2019)
29. S. Parisot et al., Disease prediction using graph convolutional networks: Application to autism Spectrum disorder and Alzheimer's disease. *Med. Image Anal.* **48**, 117–130 (2018)
30. A.S. Heinsfeld, A.R. Franco, R.C. Craddock, A. Buchweitz, F. Meneguzzi, Identification of autism spectrum disorder using deep learning and the ABIDE dataset. *NeuroImage Clin.* **17**, 16–23 (2018)
31. J. Yu, Manifold regularized stacked denoising autoencoders with feature selection. *Neurocomputing* **358**, 235–245 (Sep. 2019)
32. S. Rawat, A. Srinivasan, V. Ravi, U. Ghosh, Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. *Internet Technol. Lett.*, e232 (Sep. 2020)
33. Z. Tang, G. Srivastava, S. Liu, Swarm intelligence and ant colony optimization in accounting model choices. *J. Intell. Fuzzy Syst.* **38**(3), 2415–2423 (Jan. 2020)
34. J. Cui, D. Feng, Y. Li, Q. Tian, Research on simultaneous localization and mapping for AUV by an improved method: Variance reduction FastSLAM with simulated annealing. *Def. Technol* (Oct 2019)
35. E. Rashedi, H. Nezamabadi-pour, S. Saryazdi, GSA: A gravitational search algorithm. *Inf. Sci. (Ny).* **179**(13), 2232–2248 (Jun. 2009)
36. J.M.T. Wu, G. Srivastava, M. Pirouz, J.C.W. Lin, A GA-based Data Sanitization for Hiding Sensitive Information with Multi-Thresholds Constraint, in *Proceedings – 2020 International Conference on Pervasive Artificial Intelligence, (ICPAI 2020, 2020)*, pp. 29–34

37. O. Il-Seok, J.-S. Lee, B.-R. Moon, Hybrid genetic algorithms for feature selection. *IEEE Trans. Pattern Anal. Mach. Intell.* **26**(11), 1424–1437 (Nov. 2004)
38. J. Liang et al., Multimodal multiobjective optimization with differential evolution. *Swarm Evol. Comput.* **44**, 1028–1059 (Feb. 2019)
39. J. Kennedy, R. Eberhart, Particle swarm optimization, in *Proceedings of ICNN'95 – International Conference on Neural Networks*, vol. 4, (1995), pp. 1942–1948
40. M.E.H. Pedersen, A.J. Chipperfield, Simplifying particle swarm optimization. *Appl. Soft Comput.* **10**(2), 618–628 (Mar. 2010)
41. S. Mirjalili, S.M. Mirjalili, A. Lewis, Grey Wolf Optimizer. *Adv. Eng. Softw.* **69**, 46–61 (2014)
42. H. Faris, I. Aljarah, M. A. Al-Betar, S. Mirjalili, Grey wolf optimizer: a review of recent variants and applications, *Neural Computing and Applications*, vol. 30, no. 2. Springer London, pp. 413–435 (01-Jul-2018)
43. M. Kohli, S. Arora, Chaotic grey wolf optimization algorithm for constrained optimization problems. *J. Comput. Des. Eng.* **5**(4), 458–472 (Oct. 2018)
44. S. Mirjalili, A. Lewis, The whale optimization algorithm. *Adv. Eng. Softw.* **95**, 51–67 (May 2016)
45. P. Raja, B. Pahat, P. Raja, B. Pahat, Multi-Swarm Bat Algorithm Soft Computing and Data Mining Center, Universiti Tun Hussein Onn Malaysia College of Information Technology, Universiti Tenaga Nasional, 43000 Kajang, Selangor, Faculty of Computer Science and Information Technology, Unive, vol. 10, no. 12, pp. 1389–1395, 2015
46. N.B. Arunekumar, A. Kumar, K.S. Joseph, Hybrid bat inspired algorithm for multiprocessor real-time scheduling preparation, in *2016 International Conference on Communication and Signal Processing (ICCSP)*, (2016), pp. 2194–2198
47. E. Emary, H.M. Zawbaa, A.E. Hassanien, Binary ant lion approaches for feature selection. *Neurocomputing* **213**, 54–65 (Nov. 2016)
48. H. Sharma, G. Hazrati, J.C. Bansal, Spider monkey optimization algorithm, in *Studies in computational intelligence*, vol. 779, (Springer Verlag, 2019), pp. 43–59
49. S. Mirjalili, A.H. Gandomi, S.Z. Mirjalili, S. Saremi, H. Faris, S.M. Mirjalili, Salp swarm algorithm: A bio-inspired optimizer for engineering design problems. *Adv. Eng. Softw.* **114**, 163–191 (Dec. 2017)
50. H. Faris et al., An efficient binary Salp swarm algorithm with crossover scheme for feature selection problems. *Knowledge-Based Syst.* **154**, 43–67 (Aug. 2018)
51. I. Aljarah, M. Mafarja, A.A. Heidari, H. Faris, Y. Zhang, S. Mirjalili, Asynchronous accelerating multi-leader salp chains for feature selection. *Appl. Soft Comput. J.* **71**, 964–979 (2018)
52. S. Mirjalili, The ant lion optimizer. *Adv. Eng. Softw.* **83**, 80–98 (May 2015)
53. E. Emary, H.M. Zawbaa, A.E. Hassanien, Binary ant lion approaches for feature selection. *Neurocomputing* **213**, 54–65 (2016)
54. R. Rajabioun, Cuckoo optimization algorithm. *Applied Soft Computing* **11**, 5508–5518 (2011)
55. C. Paper, An improved cuckoo search algorithm for parallel machine scheduling Metadata of the chapter that will be visualized in SpringerLink, January, 2015
56. S. Arora, P. Anand, Binary butterfly optimization approaches for feature selection. *Expert Syst. Appl.* **116**, 147–160 (Feb. 2019)
57. K.K. Bharti, P.K. Singh, Opposition chaotic fitness mutation based adaptive inertia weight BPSO for feature selection in text clustering. *Appl. Soft Comput.* **43**, 20–34 (Jun. 2016)
58. M. Mafarja et al., Evolutionary population dynamics and grasshopper optimization approaches for feature selection problems. *Knowledge-Based Syst.* **145**, 1–14 (2018)
59. S. Mirjalili, A. Lewis, S-shaped versus V-shaped transfer functions for binary particle swarm optimization. *Swarm Evol. Comput.* **9**, 1–14 (Apr. 2013)
60. D. Binu, B.S. Kariyappa, RideNN: A new rider optimization algorithm-based neural network for fault diagnosis in analog circuits. *IEEE Trans. Instrum. Meas.* **68**(1), 2–26 (Jan. 2019)
61. K.A.K. Niazi, W. Akhtar, H.A. Khan, Y. Yang, S. Athar, Hotspot diagnosis for solar photovoltaic modules using a Naive Bayes classifier. *Sol. Energy* **190**, 34–43 (Sep. 2019)
62. M. Wadkar, F. Di Troia, M. Stamp, Detecting malware evolution using support vector machines. *Expert Syst. Appl.* **143**, 113022 (Apr. 2020)

63. M. Polato, F. Aioli, Boolean kernels for rule based interpretation of support vector machines. *Neurocomputing* **342**, 113–124 (May 2019)
64. T. Wang, Y. Qiu, J. Hua, Centered kernel alignment inspired fuzzy support vector machine. *Fuzzy Sets Syst* **394**, 110–123 (Oct 2019)
65. M.V.F. Menezes, L.C.B. Torres, A.P. Braga, Width optimization of RBF kernels for binary classification of support vector machines: A density estimation-based approach. *Pattern Recogn. Lett.* **128**, 1–7 (Dec. 2019)
66. D. Ravi, M. Bober, G.M. Farinella, M. Guarnera, S. Battiato, Semantic segmentation of images exploiting DCT based features and random forest. *Pattern Recognit* **52**, 260–273 (2016)
67. J.R. Quinlan, Induction of decision trees. *Mach. Learn.* **1**(1), 81–106 (1986)
68. S. Lomax, S. Vadera, A Survey of Cost-Sensitive Decision Tree Induction Algorithms. *ACM Comput. Surv* **45**(2), 16–16 (2013)

# Machine Learning for Fog Computing-Based IoT Networks in Smart City Environment



Subhendu Ghosh, Vinod Chandra, and Aneek Adhya

## 1 Introduction

Though the definition of smart city may not be very crystallized till date, rather leaving many opportunities for further debates and discussions, the smart city typically refers to digital and ICT-based innovation so as to provide efficient urban services and new economic opportunities for users [1]. In 2018, the overall global population was almost 7.6 billion with 55% people living in urban areas and the remaining people living in rural areas [2]. It appears that in 2050, the global population would increase to 9.8 billion with urban and rural populations of 68% and 32%, respectively [2]. Therefore, urbanization is expected to take place at an overwhelming pace. In view of addressing varying requirements of users in a smart and sustainable way in diverse fields of healthcare, agriculture, industry, energy, security, education, transportation, smart home, etc., Internet of Things (IoT) is considered to be one of the key enabling technologies. The phrase “Internet of Things” was first used by Kevin Ashton in 1999 in his presentations at Procter & Gamble (P&G) [3]. Though usage of the phrase has not started long back, the concept of “interconnected devices” has been existing since 1970s [4]. IoT primarily refers to the sensing and computing devices interconnected through the Internet. Many smart devices are connected to the Internet and execute their assigned task after analysing data collected from the physical environment [5].

Efficiency in computing and storage power is the key in the development of IoT. In this regard, cloud computing is used as an architecture to efficiently provide computing and storage resources that can be provisioned/released (on demand) with the least management effort [6]. Thus, cloud computing technology plays the

---

S. Ghosh · V. Chandra · A. Adhya (✉)  
Indian Institute of Technology Kharagpur, Kharagpur, West Bengal, India  
e-mail: [aneek@gssst.iitkgp.ac.in](mailto:aneek@gssst.iitkgp.ac.in)

principal role in IoT-based applications. IoT devices after collecting and organizing data transmit them to the application layer of the cloud computing platform. Cloud service can be delivered in three models, viz., software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) [7, 8].

- SaaS: In this type of service, software is offered in pay-per-use manner, and hosted and managed at a distance by single or multiple providers. User has no information about the infrastructure of the cloud. Google workspace, Dropbox, Salesforce, Cisco WebEx and Concur are some of the common examples of SaaS services.
- PaaS: This type of service provides application development environment to the users. Users control the applications that run in that platform, even though users do not have control on the operating system and hardware. Microsoft Azure, Heroku, AWS Lambda and Google app engine are some of the products that provide PaaS service to their customers.
- IaaS: It provides the cloud infrastructures as a service. Users can manage the servers, storage and network devices instead of purchasing servers, software, data centre space or network equipment. Some of the products that provide IaaS services are Digitalocean, Linode, Amazon web services, Cisco Metacloud, Microsoft Azure and Google compute engine.

Even though the requirement of large computing and storage power in IoT is served using cloud technology, cloud-based IoT applications face challenges in view of high latency, lack of resources, low bandwidth, absence of continuous connectivity, etc. In particular, for time-sensitive IoT applications, centralized cloud access may not be adequate. Latency plays a very important role in case of time-sensitive applications related to health care, vehicle-to-vehicle communications, etc. [9]. Due to lack of resources, some IoT devices, such as vehicles and drones, may not be able to set up direct connection to the cloud. An interim layer device is required to solve computing resource limitation and cloud-IoT device protocol mismatch issues [10]. In general, high bandwidth is required to transfer data from IoT devices to cloud, since IoT devices typically generate huge amount of data. Sending all data to cloud may not be necessary, and data generated at the edge of the network layer should be locally processed instead of sending it to the cloud [10]. Some moving devices, such as cars and drones may experience network fluctuation, and therefore, providing continuous cloud service may become very challenging.

In order to mitigate the disadvantages of cloud computing, fog computing-based IoT architecture is introduced. Fog computing extends resources like processing, memory and storage, which were earlier available only with cloud, to the end devices. Cloud computing services, such as SaaS, PaaS and IaaS, can be extended with fog computing. The end devices, such as sensors, controllers and actuators (e.g., smartphones, tablets and smart watches), are placed at the bottom of the architecture. Fog computing layer consisting of access points, switches, gateways, routers, etc. is set up above the end devices. Conventional cloud servers and cloud data centres are placed at the top. Fog computing offers lower latency, large-

scale geographical distribution, lower network bandwidth requirement, improved flexibility, heterogeneity and scalability [9].

In order to support advanced, intelligent services, large volumes of heterogeneous data are generated with different time stamps from different IoT devices positioned at different locations. The data may remain contaminated with high noise. Use of traditional methods or algorithms for extraction of hidden information from the large data may not be efficient. In this regard, new procedures and algorithms are needed to support advanced services [11]. Machine learning (ML) assists in data processing and making inferences for the devices, thereby enabling them to change state or interact according to the extracted knowledge [12, 13]. In recent times, ML algorithms are used in many smart city-related IoT applications, such as smart transportation, health care, security, agriculture, weather forecasting and environment monitoring. ML can be used in optimizing the usage of computing resource, bandwidth and energy consumption. ML is also used to support different delay-sensitive services used in the domain of healthcare and autonomous driving.

In this chapter, various topics are presented as follows. In Sect. 2, we explore layered architecture for conventional and fog computing-based IoT networks. Thereafter in Sect. 3, a concise introduction of different ML algorithms is presented. In Sect. 4 we present a review of recent literature that adopt ML algorithms in different aspects of cloud- and fog-based IoT applications to be used in smart city environment. In particular, we present different examples of ML-based IoT applications for smart city environment, and use of ML in computing and resource management, decision making and security. Finally, we conclude the chapter in Sect. 5.

## 2 IoT Architecture

We describe the layered IoT architecture in the following.

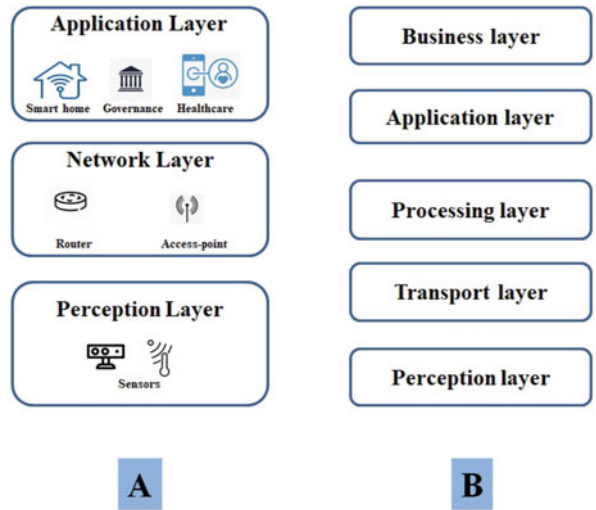
### 2.1 Three-Layer Architecture

IoT architecture primarily consists of three layers (Fig. 1), viz., perception layer, transmission layer and application layer [14, 15].

- (1) Perception Layer: It is the bottom-most layer of IoT architecture, which contains heterogeneous types of physical devices, such as sensors, actuators and controllers [14]. Using different devices, such as RFID readers, quick response (QR) code, global positioning system (GPS) devices, bluetooth devices, light/humidity/temperature sensors, etc., data is collected, detected and processed from the environment, and thereafter transmitted to the network layer.



**Fig. 1** IoT architecture: (a) Three layer, (b) Five layer [15, 17]



- (2) **Network Layer/Transmission Layer:** This layer works as transport section to connect the perception layer to the application layer. It sends data collected by the perception layer to the information processing unit in the upper layer [14]. The primary function of this layer is routing and transmission of data. This layer integrates computing platforms, networking devices such as routers, switches and Internet gateways, and communication technologies such as WiFi, LTE and bluetooth [15, 16].
- (3) **Application Layer:** It lies at the top of the IoT architecture, and provides required services using the data from the network layer. It provides various enterprise services and intelligent processing over the data depending on different applications like health care, agriculture and industry [14, 16].

## 2.2 Five-Layer Architecture

Three-layer architecture is the basic IoT architecture, and may not be sufficient when finer aspects of modern technologies are integrated in the IoT. Two additional layers, viz., processing layer and business layer, are added with the existing three-layer architecture (Fig. 1) [15, 17]. Perception (or physical) layer senses data about the physical world. Transport layer assists to transfer the data sensed by the sensors to the processing layer, and in the reverse direction as well, using wireless/wired networks. Processing layer analyses, stores and processes the data arriving from the transport layer. It may employ technologies like databases, cloud computing and big data processing [15]. Application layer provides desired service according to the application type. The entire IoT model is controlled by the business

layer, which manages all application and privacy-related issues in a business and profit model [15, 17]. Some literature also use even higher (i.e., more than five) number of architecture layers for complex IoT systems and applications in order to systematically address different IoT building blocks, components and their mutual interactions [17].

### ***2.3 Fog-Based IoT Architecture***

For fog-based IoT architecture, four additional layers, namely, the monitoring, preprocessing, temporary storage and security layers, are modelled in between the physical layer and the transport layer [9, 15, 17]. Monitoring layer performs monitoring of resources allocated to the nodes, responses of the nodes and services [15, 17]. Preprocessing layer enables data analysis, filtering and trimming to obtain information from the data [9]. Temporary storage layer provides temporary storage, data duplication, etc. for preprocessed data, if required. However, the data that need to be sent to the cloud is not stored in this layer. Security layer adopts different actions to ensure security and privacy of data. Thus, fog nodes provide monitoring, preprocessing, temporary storage and security service for sensor data.

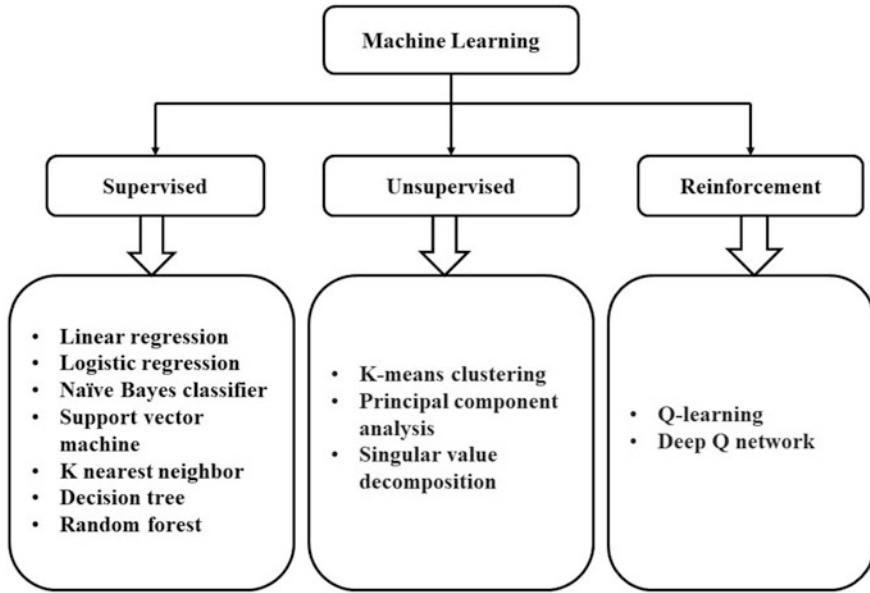
## **3 Machine Learning in IoT Application**

In recent times, ML is being integrated in many IoT applications for computing and data analysis. The primary objective of ML is to learn from data without explicit programming. ML is a sub-field of artificial intelligence (AI), where AI is the human like learning and decision-making ability of machines enabled through intelligent programming. To achieve the goals of reasoning, learning and perceiving, AI uses tools like mathematical optimization, logic and probability [18]. Deep learning belongs to the vast family of ML algorithms that functions like human brains. Deep learning is implemented with many hidden layers in artificial neural networks (ANNs) [18, 19].

ML algorithms are broadly categorized into three classes, viz., supervised, unsupervised and reinforcement learning (Fig. 2). A brief description about these algorithms is presented in the following.

### ***3.1 Supervised Learning***

In supervised learning, the true labels are assigned to input datasets, and algorithms are trained on the labelled dataset. A supervised learning algorithm inspects the training data, and creates a generalized function, which is used to map new inputs to



**Fig. 2** Classification of ML algorithms

predict the output values. In ML algorithms, during training phase, a cost function is optimized, where the cost function represents the difference between the predicted output value and the true output value. The cost function value is considered as a measure of performance of an ML model. Minimization of cost function is required during training the ML model so that the model can predict the correct output value. Supervised learning models can be used for regression as well as classification. In regression, the algorithms predict a continuous real value, whereas in classification the algorithms predict the class of an input dataset. Some of the widely used supervised learning algorithms are discussed in the following.

**Linear Regression:** It is a statistical technique that assesses the relation between a given input and the related output. A mapping from input to a continuous function is done in this model. Let a training dataset comprises of  $M$  labelled examples  $(\mathbf{X}, Y \in R^{N+1})$ , where  $\mathbf{X}$  and  $Y$  are the independent and dependent variables, respectively, and  $N$  represents the number of features in each example. Linear regression model considers the linear relation between  $\mathbf{X}$  and  $Y$  and is represented by the following Hypothesis function:

$$H(\mathbf{X}) = W_0 + W_1X_1 + W_2X_2 + \dots + W_NX_N \quad (1)$$

where  $W_0, W_1, W_2, \dots, W_N$  are the weights of the model and  $X_1, X_2, \dots, X_N$  are the input feature vectors. Equation (1) represents multivariate regression model, where the weights are evaluated using different optimization methods [20].

**Logistic Regression:** Linear regression models are ideal for evaluating continuous output. In classification tasks a discrete output is required. In order to predict binary classes logistic regression is used, even though logistic regression can be used to predict more than two classes. Logistic regression predicts the probabilities of output variables, and the related Hypotheses function is given by

$$H(\mathbf{X}) = S(W_0 + W_1X_1 + W_2X_2 + \dots + W_NX_N) \quad (2)$$

where  $S(Z)$  represents the Sigmoid function, which is represented by  $S(Z) = \frac{1}{1+\exp(-Z)}$  with output values lying between 0 to 1 [19].

**Naive Bayes (NB) Classifier:** This classifier can be easily trained based on Bayes' rule, and it calculates the probability of an outcome. The term 'Naive' is used to indicate that these algorithms use the assumption that the occurrence of certain features is independent of the occurrence of other features, leading to less efficiency, even though improved speed compared to other existing supervised ML algorithms [21].

**K Nearest Neighbour (KNN):** KNN is one type of instance based learning. In instance based learning the training examples are memorized, and when there is a new instance, the algorithm compares it with the stored examples, and depending on the similarity a target value is given. KNN algorithms consider all instances as points in the  $N$  dimensional space  $R^N$ , and Euclidean distance is used as the measure of the nearest neighbour [22].

**Support Vector Machine (SVM):** SVM algorithms search a hyperplane in  $N$  dimensional space, where  $N$  is the number of features in input vector. Even though many separate hyperplanes can be selected to distinguish between two data points, we need to select the hyperplane with the maximum separating distance from the two data points [23].

**Decision tree:** This algorithm can be used for both regression and classification tasks; but the algorithm is preferred for classification. It has a structure like a tree. The features of a dataset are represented by internal nodes, decision rules are used to construct branches and outcomes are represented by leaf nodes. Decision tree contains two types of nodes: decision nodes and leaf nodes. Decision nodes take decision and have multiple branches, and leaf nodes represent the outcomes. A decision tree is initiated from the root node, and extended to branches. Hierarchical set of rules are framed so as to divide a large dataset into smaller data segments [19, 24, 25].

**Random forest (RF):** RF belongs to ensemble supervised ML algorithms, wherein ensemble learning refers to the method to combine multiple classifiers so as to solve an ML task, thereby increasing its performance. An RF classifier is a combination of multiple decision tree classifiers. During training phase an RF algorithm generates multiple trees from a given dataset. In order to classify the object for a given input vector, all trees in the forest individually process the input vector. Each tree obtains

the classification outcome. Taking into consideration all trees, the forest selects the outcome with the maximum number of favourable responses [26, 27].

### 3.2 *Unsupervised Learning*

In unsupervised learning algorithms there is no labelled input datasets. The algorithms find out hidden structures from the input data and make inferences. In this type of tasks the input feature vectors are given, and the similarities are required to be determined. Popular algorithms related to unsupervised learning are the K-means clustering, principal component analysis and singular value decomposition.

**K-Means Clustering:** In these algorithms, the dataset is divided into  $K$  different clusters with one definite cluster centre (or centroid) per cluster, and every object in the dataset is considered to be a part of a particular cluster. The primary objective of the algorithm is to find the centroids. During clustering the distance between each object and each centroid is calculated, and the object is allocated to the cluster with the minimum distance. After computation of distances for all objects, a new set of centroids is defined, and again all the distances are recalculated. This process iterates until the required tolerance level is achieved [21, 28].

**Principal Component Analysis (PCA):** PCA is frequently applied in reducing the dimension of a large dataset, and it transforms higher number of variable space into a lower one preserving the most of the information. It uses an orthogonal transformation to convert a correlated set of variables into an uncorrelated set of variables, which are called the principal components representing the directions of the maximum variances [29, 30].

**Singular Value Decomposition (SVD):** It is one of the most familiar unsupervised learning algorithms used for feature reduction in a dataset. SVD basically factorizes any given matrix into three matrices, and for a matrix  $A$  the SVD is given as,

$$A = U \Sigma V^T \quad (3)$$

where  $A$  represents  $(m \times n)$  matrix,  $U$  represents  $(m \times m)$  orthogonal matrix,  $\Sigma$  represents  $(m \times n)$  non-negative diagonal rectangular matrix, and  $V$  represents  $(n \times n)$  orthogonal matrix.  $U$  and  $V$  are known as the left and right singular vectors, respectively, and diagonal elements of  $\Sigma$  are the singular values [31, 32].

### 3.3 *Reinforcement Learning*

In reinforcement learning algorithms the main objective remains to identify the actions to be taken in a dynamic environment to maximize the reward. The learner

or agent is not aware of the best action to be taken, but inspects the action that would produce more rewards. The action to be taken influences the current reward as well as the next states. The two main features of reinforcement learning algorithms are the trial-and-error investigation and the delayed reward [33]. There are mainly two types of reinforcement learning algorithms based on the methods used by the learner to decide its action, namely the model-free and model-based. In model-free reinforcement learning algorithms, learner estimates the optimal policy without using or estimating the dynamics of the environment, rather directly learning from the real environment. However, in the model-based reinforcement learning algorithms, the learner aims to construct a model from the interaction with the real environment, and tries to predict the optimal policy and future reward from the constructed model.

**Q-learning:** Q-learning algorithm is one of the most popular model-free reinforcement learning algorithm, where the learner learns the optimal policy based on the rewards received by taking different actions in different states of the environment with the objective to maximize the overall reward [34]. The learner checks the received reward for the action taken at each state, and updates the Q-value for the corresponding state-action pair. A higher Q-value implies better chances of receiving greater rewards. As Q-values need to be stored for each state-action pair, Q-learning algorithm is generally used for discrete, small to medium size environments. In a continuous environment, Q-learning algorithm may be used by discretizing the states.

**Deep Q-learning (DQN):** DQN is also a model-free learning algorithm, where it finds the optimal policy using a deep neural network [35]. DQN generally handles large environments that involve continuous (and/or discrete) actions and states. DQN uses deep neural network to approximate the Q-values. At any given time, the state of the environment is given as input to the deep neural network, and the Q-values of all possible actions are predicted as the output.

## 4 ML-Based IoT Applications

In this section we present different examples of ML-based IoT applications for smart city environment, and use of ML in computing and resource management, decision making and security.

**Table 1** Example of ML-Based IoT Applications

Ref.	Application	ML Algorithm	Data	Accuracy (%)
[36]	Arrhythmia classification	RF	ECG signal	96
[37]	Crop health monitoring	NB, SVM and NN	IoT sensor data and drone image data	NB: 84 SVM: 78 NN: 98.4
[38]	Air quality prediction	Decision tree regression, RF regression and gradient boosting regression	Meteorological parameters (including PM2.5 concentration)	–
[39]	Classification of roadway obstacles	Soft margin SVM, sparse soft margin SVM, logistic regression, adaboost with stumps and RF	Smartphone's GPS and accelerometer data	–
[40]	Waste management	K-means clustering (Elbow method) and logistic regression	Geographic locations and status of trash bins	–

#### 4.1 Example of ML-Based IoT Applications for Smart City Scenario

Table 1 shows different IoT applications with focus on ML algorithms used, data over which ML algorithms are used and accuracy (%) of the ML algorithms. Arrhythmia is related to atypical heart beat with too fast or too slow or irregular heart beating. Continuous monitoring of heart beat is required in diagnosing this type of patients to prevent heart diseases. Devadharshini et al. use IoT and ML to monitor arrhythmic patients and classify them depending on the abnormality [36]. Electrocardiogram (ECG), pulse rate and body temperature of patient are measured using wearable sensors, and these physical parameters are transmitted using mobile application and stored in the cloud. After accessing the patients' ECG data from cloud, the mobile application processes it to suggest the patients' arrhythmia condition. RF algorithm is used to classify arrhythmia conditions into 16 categories with 96% accuracy. Shafi et al. explore an IoT-based infrastructure to monitor crop health [37]. Air temperature and humidity sensor, and soil temperature and soil moisture sensor are used as IoT nodes (equipped with solar cells) to monitor the environmental conditions. The IoT nodes forward the captured data at regular intervals (typically 5 minutes) to the local server. A multispectral camera mounted on a drone also captures images of the crops typically once in a week. Data generated from multiple sources are mapped following common temporal resolution, and thereafter datasets are labelled to run the following supervised ML algorithms: NB, SVM and neural network (NN). The crops are classified into three

classes: unhealthy, stressed and healthy. The accuracy of NB, SVM and NN models are shown as 84%, 78% and 98.4%, respectively.

Ameer et al. show relative performance of different ML models used for air quality prediction in smart cities [38]. PM2.5 particles are tiny particles with diameter less than 2.5  $\mu\text{m}$ . The particles are very light and remain suspended in air for a longer time compared to other heavier suspended particles. The particles possess larger risk in view of entering human respiratory system, and air quality index (AQI) is measured depending on PM2.5 particle concentration in air. In this study, air pollutants are measured using IoT sensors kept at different locations in five different cities. Their dataset comprises 15 meteorological parameters, including the PM2.5 concentration. The study predicts air quality using different supervised ML techniques, e.g., decision tree, RF and gradient boosting regression. The performance is estimated in terms of the processing time, mean absolute error (MAE) and root mean squared error (RMSE). RF is shown to be the best algorithm for air quality prediction. Brisimi et al. explore ML-based roadway obstacle detection and classification (e.g., location and identification of street bumps) method for smart vehicular traffic transport system [39]. A person driving a vehicle uses a smartphone, and keeps track of the information like longitude-latitude and speed of the vehicle obtained through the smartphone's GPS and accelerometer data. These data are transmitted to a remote server for further processing. For classification purpose, supervised algorithms, such as soft margin SVM, sparse soft margin SVM, logistic regression, adaboost with stumps and RF algorithms are used. In [40], smart management method for waste disposal is discussed so as to keep city environment clean and healthy. Open source data of garbage bins are checked, and the garbage bin status is shared to garbage removing vehicles. The authors use an intelligent method offering automatic classification of trash bin locations, and predict waste accumulation status of the trash bins. Thereafter, optimized vehicles routes for garbage trucks are identified. Elbow method is used for unsupervised K-means clustering problem, while logistic regression is used for trash bin status prediction.

## ***4.2 Machine Learning in Computing and Resource Management***

In Table 2 we present several studies that use ML algorithms to improve computing and resource management in IoT applications. Yan et al. propose an intelligent transportation system comprising fog computing-based vehicular network, where vehicles ask for content files stored in cache storage of fog-access points (F-APs) and/or other vehicles [41]. The contents are transmitted using wireless channels through F-AP mode or vehicle-to-vehicle (V2V) mode. The authors propose a mixed integer non-linear programming (MINLP)-based optimization formulation to jointly optimize the access mode selection and bandwidth allocation. Due to high computational complexity, the original problem is divided into two subproblems.



**Table 2** ML in computing and resource management

Ref.	Application	Related Issue	ML Algorithm	Data
[41]	Fog-based vehicular network	Access mode selection and bandwidth allocation	Q-learning	Request for content file
[42]	City surveillance	Latency, storage and bandwidth requirement	LBPH	Video
[43]	Workers' health status monitoring in maritime environment	Response time and bandwidth utilization	ANN	Human physical parameters collected by WBSN
[44]	MEC-based IoT network	Mobility aware, energy-efficient server allocation	Deep learning	Traffic (job) request
[45]	Cloud management system	Server allocation	SVRT	Cloud workload data
[46]	Heterogeneous fog-based IoT network	Energy consumption reduction	Reinforcement learning	CPU and memory usage

A Q-learning algorithm is used for the first subproblem, i.e., the selection of access mode in absence of global information, whereas the second subproblem, i.e., the optimal spectrum allocation, is solved using convex optimization. Proposed method offers improved performance in terms of expected data rate and sum payoff compared to the existing methods. Paolo et al. present a face recognition system for smart city video surveillance application [42]. An architecture that supports ML model distributed among edge nodes and cloud in a collaborative edge computing architecture is proposed. For this purpose, an ML model based on local binary patterns histogram (LBPH) algorithm is used. In order to reduce latency, storage and bandwidth requirement, video streams are not transmitted to centralized cloud; instead the streams are processed in real-time at the edge network using the distributed ML model.

Abedi et al. propose an AI-based algorithm for task distribution between fog and cloud servers to monitor workers' health condition in maritime environment [43]. Wireless body sensor networks (WBSNs) collect human physical parameters, and send them to an entity referred to as broker. It analyses the tasks and send them to fog or cloud servers for fog/cloud computing so as to predict human body condition in different environments and working conditions. The proposed algorithm uses ANN, and offers improved response time compared to only cloud-based and only fog-based approaches. In terms of Internet bandwidth utilization efficiency, the algorithm offers improved performance compared to only cloud-based approaches; however, it offers inferior performance compared to only fog-based approaches. Zaiwar et al. explore a method for the allocation of optimal server and the resource

(virtual machines or VMs) in the server for a dynamic traffic (i.e., job) request from a UE in a mobile edge computing (MEC)-based IoT network [44]. As dynamic traffic requests arrive in the MEC servers, resources are allocated in an intelligent way so as to meet the QoS requirement. In this regard, a mobility aware energy efficient resource allocation algorithm is proposed based on deep learning. The algorithm uses UE-related data (e.g., requested resource amount, location and time), resultant reward and energy efficiency of servers to allocate resources with high (greater than 70%) accuracy. In [45], a prediction method for optimized use of cloud resources is presented. As cloud workloads and resource utilization are highly dynamic and often become unstable, a prediction method to forecast cloud resource usage is required. The knowledge allows cloud management system to decide when a server becomes overloaded, leading to immediate migration of VMs from the overloaded server to an underutilized server. Resource workload data in terms of different attributes, such as CPU utilization, memory utilization, disk read/write throughput, and network transmit/receive throughput, are collected from different sources, e.g., Google cluster workload traces, Bitbrains service provider. Support vector regression technique (SVRT), which is a regression technique designed based on SVM, is used to predict resource utilization. In [46], a reinforcement learning-based ML model is used to reduce energy consumption in heterogeneous fog-based IoT network. The network density, latency and mobility are used as the design constraints. The authors show that using the ML model the workload in terms of the CPU and memory usage is effectively reduced compared to the case without using it, thereby effectively reducing the energy demand.

### 4.3 *Machine Learning in Decision Making*

In Table 3 we show several studies that use ML algorithms to improve decision making ability for IoT-based smart city applications. In [47], Diedrichs et al. propose an ML-based frost prediction methodology for IoT-based weather forecasting application. Frost can severely damage crop fields, and preventive measures such as using air heaters by burning fuels (diesel, petrol, gas, etc.) are very expensive. Frost is a local event and may partially impact a crop field; however, it may significantly damage the production. On the other hand, adequate amount of historical data may not be available since fog events do not occur often in a year. Thus, it is difficult to predict occurrence of a frost event. If frost event is not predicted accurately, either the crop production is damaged or fuel burning becomes useless. In the proposed method, weather stations equipped with Internet-enabled weather data collection devices first provide historical data (temperature and humidity sensor data) to prediction engine to train the ML model, and then send new data to improve the prediction model. Bayesian network, logistic regression, binary trees and RF algorithms are used for decision making. In [48], Yahyaoui et al. present a medical decision support to predict diabetes, which is a major causes of death in the world as per World Health Organisation (WHO) report. Medical decision

**Table 3** ML in decision making

Ref.	Application	Related Issue	ML Algorithm	Data
[47]	Weather forecasting	Frost prediction	Bayesian network, logistic regression, binary trees and RF	Temperature and humidity
[48]	Diabetes prediction	Clinical decision making	SVM,RF and CNN	Online diabetes dataset
[49]	Autonomous vehicle driving	Control of traffic light	BRL	Number of vehicles and waiting times at intersections
[50]	Spectrum management	Dynamic spectrum sharing	Gradient boosting tree algorithm	Power levels of various channels
[51]	Autonomous vehicle driving	Overtaking decision on highway	DRL	Highway environment data
[52]	River flood severity	Water level prediction	ANN, RF, SVM, KNN and LSTM	Flood sensor data

support system shows its effectiveness in clinical decision making for medical consultants. The decision system is based on SVM, RF and convolutional neural network (CNN) algorithms. These algorithms are processed on online PIMA Indians diabetes dataset comprising 768 examples and 8 features. The accuracy of diabetes prediction obtained using CNN, SVM and RF algorithms are 76.81%, 65.38% and 83.67%, respectively. In [49], broad reinforcement learning (BRL) model is used to support IoT-based autonomous driving system. Proposed model combines the broad learning system with a reinforcement learning paradigm for improved efficiency and accuracy of modelling and decision making. Data regarding the number of vehicles and their waiting times are used in the proposed model to manage the traffic flow and decrease the waiting times of vehicles at the intersections of smart cities by autonomously controlling the traffic lights. Li et al. present IoT-enabled ML-based decision approach for next-generation regulatory spectrum management [50]. The fog node gathers the power level data from various sensors, and analyses it to determine the spectrum occupancy. It uses the reinforcement learning-based gradient boosting tree algorithm, and the average prediction accuracy is shown to be 95%.

Autonomous vehicle driving is expected to be widely deployed in smart city environment. Liao et al. propose an autonomous vehicle driving strategy on highways using offline, highway environment data [51]. Deep reinforcement learning (DRL)-based duelling DQN algorithm is explored to suggest overtaking decision on highways. In [52], an intelligent river water level prediction and flood severity model is proposed. Flood sensor data from different flood monitoring centres of various countries are used in determining the water levels. From each sample in these dataset, 11 features such as monsoonal rain, number of dead, number of displaced, heavy rain and affected area are extracted. ANN, RF, KNN classifier, SVM and Long-Short Term Memory (LSTM) algorithms are used.

#### 4.4 *Machine Learning in Security*

In IoT networks the security and reliability are two important issues for different services offered by the service provider. To maintain security and reliability trust is required among different devices in the fog network. There are various security levels of fog computing wherein different ML solutions can be used to improve the overall security and reliability performance of the system. The security levels can be categorized into device security, network security and data security [53]. In Table 4, we show applications of ML for security in fog computing based IoT networks. Fadlullah et al. propose an early warning system against malicious activities, such as distributed denial of service (DDoS) attacks and abnormal voltage surge for smart grid systems [54]. Authentication requests from smart meters, and power, voltage and current data are processed. The data learning about malicious attack events are modelled through a Gaussian process which helps the control centre to forecast occurrence of future events in the network. Since the Gaussian processes offer a principled, probabilistic approach to facilitate ML, the same is used here for early warning system design. The proposed model mitigates the malicious events. In [55], the authors use a method to detect attack in smart grid system. The proposed method employs state vector estimation in which initially the state of the system is estimated from the observed measurements. Thereafter the residual between the observed and estimated measurements are computed, from which data injection attack is identified. The authors also propose supervised learning algorithm to predict false data injection (FDI) attacks. Power, voltage and current data from IEEE 9-bus, 57-bus and 118-bus test database are used. It is empirically shown that the statistical learning algorithms have better performance of attack detection than those employing SVM methods. In [56], the authors analyse three supervised learning techniques, viz., SVM, KNN and ANN, along with different feature selection techniques (e.g., genetic algorithm, particle swarm optimization) to detect FDI attacks targeting smart grids. The accuracy of SVM and KNN algorithms is found to be more than that of ANN, and it is proved that the proposed ML methods are successful in detecting FDI attacks, which is nearly impossible with currently available data detection systems.

In [57], the authors propose a scheme to protect user data privacy in healthcare system. Raw sensory data often contains sensitive user information which may pose a serious security threat. In this paper a multifunctional data aggregation method with differential privacy is proposed. The methods offer an accuracy of 90%. Proposed architecture lessens the burden on the cloud server by reducing the amount of data required to be sent to it. The paper uses patient's data from reference energy disaggregation dataset (REDD) and mobile health (MHEALTH) dataset. The learning model answers the aggregation queries to predict outcome. Using differential privacy policy, this model effectively prevents data breaches and loss. Zisis et al. propose an autonomic self-protecting system in maritime environment employing SVM ML models that are employed at the edge of the cloud [58]. The ML model enables unsupervised learning with low footprint of

**Table 4** ML in Security

Ref.	Type of attack	Security level	ML Algorithm	Data	Application
[54]	DDoS and abnormal voltage surges	Authentication and availability	Gaussian process regression	Authentication requests from smart meters, power, voltage and current	Network security in smart grid
[55]	Spoofing and FDI	Authentication	SVM	Power, voltage and current	Network security in smart grid
[56]	FDI	DoS	SVM, KNN and ANN	Power, voltage and current	Network security in smart grid
[57]	Data loss	User data privacy	Multifunctional data aggregation	Patient's data from REDD and MHEALTH datasets	Data security in healthcare
[58]	Spoofing, modification, interception, impersonation, substitution, eavesdropping, session hijacking, wiretapping	Data confidentiality, integrity and availability	SVM	System transponder data	Data security in maritime systems
[59]	Intrusion	Misuse and anomaly detection	SVM and ANN	NetFlow data	Cyber security

system transponder data from sensors in the perception layer for anomaly detection. The proposed method preserves the confidentiality, integrity and availability of data by curtailing various attacks, like sensor spoofing, interception, impersonation, eavesdropping, wiretapping and session hijacking. Three different types of cyber analytic are available in intrusion detection system (IDS), namely, misuse-based, anomaly-based and hybrid. It is shown in [59] that for NetFlow data from Internet, various ML techniques, such as SVM and ANN, are quite effective in both the misuse and anomaly detection, offering more than 84% attack detection.

## 5 Conclusions

This chapter begins with an introduction of fog-cloud based IoT applications for smart city environment. Cloud-based IoT architectures suffer from different issues, such as high latency, large bandwidth requirement and insufficient computational

resources, that can be solved with the introduction of fog layer. Furthermore, to enable the IoT devices for intelligent decision making and improved computational efficiency ML algorithms are implemented. We briefly discuss different ML algorithms which are frequently used in different IoT-based applications. We also review different studies related to ML-based IoT applications for smart city scenario, with focus on use of ML in computing, resource management, decision making and security. These literature show that ML is very powerful tool which is presently being applied in different layers of IoT networks in smart city environment to mitigate different complex issues.

## References

1. OECD 2020, Smart Cities and Inclusive Growth [Online]. Available: [http://www.oecd.org/cfe/cities/OECD\\_Policy\\_Paper\\_Smart\\_Cities\\_and\\_Inclusive\\_Growth.pdf](http://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf). Accessed: 31 Jan 2021
2. H. Ritchie, M. Roser, Urbanization [Online]. Available: <https://ourworldindata.org/urbanization#how-many-people-will-live-in-urban-areas-in-the-future>. Accessed: 31 Jan 2021
3. K. Ashton, That ‘internet of things’ thing, *RFiD J.* **22**, 97–114 (2009)
4. K.L. Lueth, Why the Internet of Things is called Internet of Things: definition, history, disambiguation [Online]. Available: <https://iot-analytics.com/internet-of-things-definition/#:~:text=The%20birth%20of%20IoT&text=But%20the%20actual%20idea%20of,during%20his%20work%20at%20Procter-%26Gamble>. Accessed: 06 Jan 2021
5. A. Rahman, H. Hussein, Internet of Things (IoT): research challenges and future applications. *Int. J. Adv. Comput. Sci. Appl.* **10**(6), 77–82 (2019)
6. P. Mell, T. Grance, The NIST definition of cloud computing, *National Institute of Standards and Technology* (2011), pp. 1–7
7. J. Srinivas, K. Venkata, S. Reddy, Dr. A. Moiz Qyser, Cloud computing basics. *Int. J. Adv. Res. Comput. Commun. Eng.* **1**, 343–347 (2012)
8. V. Kumar, A.A. Laghari, S. Karim, M. Shakir, A.A. Brohi, Comparison of fog computing & cloud computing. *Int. J. Math. Sci. Comput.* **1**, 31–41 (2019)
9. H. Atlam, R. Walters, G. Wills, Fog computing and the internet of things: a review. *Big Data Cogn. Comput.* **2**(2), 1–18 (2018)
10. M.D. Donno, K. Tange, N. Dragoni, Foundations and evolution of modern computing paradigms: cloud, IoT, edge, and fog. *IEEE Access* **7**, 150936–150948 (2019)
11. V. Porkodi, D. Yuvaraj, J. Khan, S.A. Karuppusamy, P.M. Goel, M. Sivaram, A survey on various machine learning models in IoT applications, in *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (2020), pp. 1–4
12. F. Samie, L. Bauer, J. Henkel, From cloud down to things: an overview of machine learning in internet of things. *IEEE Internet Things J.* **6**(3), 4921–4934 (2019)
13. F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **22**(3), 1686–1721 (2020)
14. B. Gupta, M. Quamara, An overview of internet of things (IoT): architectural aspects, challenges, and protocols. *Concurrency Comput.: Pract. Exp.* **32**(21), 1–24 (2018)
15. P. Sethi, S.R. Sarangi, Internet of things: architectures, protocols, and applications. *J. Electr. Comput. Eng.* **2017**, 1–25 (2017)
16. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **4**(5), 1125–1142 (2017)

17. N.M. Kumar, P.K. Mallick, The internet of things: insights into the building blocks, component interactions, and architecture layers. *Proc. Comput. Sci.* **132**, 109–117 (2018)
18. P. Ongsulee, Artificial intelligence, machine learning and deep learning, in *2017 15th International Conference on ICT and Knowledge Engineering (ICT KE)* (2017), pp. 1–6
19. M. Gopal, *Applied Machine Learning* (McGraw-Hill, Chennai, 2018)
20. U.S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, M. Stanley, A brief survey of machine learning methods and their sensor and iot applications, in *2017 8th International Conference on Information, Intelligence, Systems Applications (IISA)* (2017), pp. 1–8
21. G. Bonaccorso, *Machine Learning Algorithms* (Packt Publishing, Birmingham, 1997)
22. T.M. Mitchell, *Machine Learning*. (McGraw Hill, New York, 1997)
23. V. Jakkula, Tutorial on Support Vector Machine (SVM) [Online]. Available: <https://course.ccs.neu.edu/cs5100f11/resources/jakkula.pdf>. Accessed: 03 Jan 2021
24. G. Bonaccorso, *Machine Learning Algorithms: A Reference Guide to Popular Algorithms for Data Science and Machine Learning* (Packt Publishing, Birmingham, 2017)
25. M. Kubat, *An Introduction to Machine Learning* (Springer, Cham, 2017)
26. V.Y. Kulkarni, P.K. Sinha, Pruning of random forest classifiers: a survey and future directions, in *2012 International Conference on Data Science Engineering (ICDSE)* (2012), pp. 64–68
27. C. Zhang, Y. Ma, *Ensemble Machine Learning: Methods and Applications* (Springer Publishing Company, Incorporated, Boston, 2012)
28. A. Kassambara, *Practical Guide to Cluster Analysis in R, Unsupervised Machine Learning* (Statistical Tools for High Throughput Data Analysis, 2017)
29. A. Tharwat, Principal component analysis – a tutorial. *Int. J. Appl. Pattern Recogn.* **3**, 1–41 (2016)
30. E. Alpaydin, *Introduction to Machine Learning* (The MIT Press, Massachusetts, 2014)
31. Z. Zhang, The singular value decomposition, applications and beyond. *CoRR*, abs/1510.08532 (2015), arXiv: 1510.08532 [Online]. Available: <http://arxiv.org/abs/1510.08532>
32. P. Dangeti, *Statistics for Machine Learning* (Packt Publishing Ltd., Birmingham, 2017)
33. R.S. Sutton, A.G. Barto, *Reinforcement Learning: An Introduction* (The MIT Press, Cambridge, MA, 2018)
34. C.J.C.H. Watkins, Learning from delayed rewards (1989)
35. V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, M. Riedmiller, Playing atari with deep reinforcement learning (2013), arXiv preprint arXiv:1312.5602
36. M.S. Devadharshini, A.S. Heena Firdaus, R. Sree Ranjani, N. Devarajan, Real time arrhythmia monitoring with machine learning classification and IoT, in *2019 International Conference on Data Science and Engineering (ICDSE)* (2019), pp. 1–4
37. U. Shafi, R. Mumtaz, N. Iqbal, S.M.H. Zaidi, S.A.R. Zaidi, I. Hussain, Z. Mahmood, A multi-modal approach for crop health mapping using low altitude remote sensing, internet of things (IoT) and machine learning. *IEEE Access* **8**, 112708–112724 (2020)
38. S. Ameer, M.A. Shah, A. Khan, H. Song, C. Maple, S.U. Islam, M.N. Asghar, Comparative analysis of machine learning techniques for predicting air quality in smart cities. *IEEE Access* **7**, 128325–128338 (2019)
39. T.S. Brisimi, C.G. Cassandras, C. Osgood, I.C. Paschalidis, Y. Zhang, Sensing and classifying roadway obstacles in smart cities: the street bump system. *IEEE Access* **4**, 1301–1312 (2016)
40. D.D. Vu, G. Kaddoum, A waste city management system for smart cities applications, in *2017 Advances in Wireless and Optical Communications (RTUWO)* (2017), pp. 225–229
41. S. Yan, X. Zhang, H. Xiang, W. Wu, Joint access mode selection and spectrum allocation for fog computing based vehicular networks. *IEEE Access* **7**, 17725–17735 (2019)
42. P. Bellavista, P. Chatzimisios, L. Foschini, M. Paradisioti, D. Scotece, A support infrastructure for machine learning at the edge in smart city surveillance, in *2019 IEEE Symposium on Computers and Communications (ISCC)* (2019), pp. 1189–1194
43. M. Abedi, M. Pourkiani, Resource allocation in combined fog-cloud scenarios by using artificial intelligence, in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)* (2020), pp. 218–222

44. Z. Ali, S. Khaf, Z.H. Abbas, G. Abbas, F. Muhammad, S. Kim, A deep learning approach for mobility-aware and energy-efficient resource allocation in MEC. *IEEE Access* **8**, 179530–179546 (2020)
45. L. Abdullah, H. Li, S. Al-Jamali, A. Al-Badwi, C. Ruan, Predicting multi-attribute host resource utilization using support vector regression technique. *IEEE Access* **8**, 66048–66067 (2020)
46. M.V. Prakash, V. Porkodi, S. Rajanarayanan, M. Khan, B.F. Ibrahim, M. Sivaram, Improved conservation of energy in fog IoT services using machine learning model, in *2020 International Conference on Computing and Information Technology (ICCIIT-1441)* (2020), pp. 1–4
47. A.L. Diedrichs, F. Bromberg, D. Dujovne, K. Brun-Laguna, T. Watteyne, Prediction of frost events using machine learning and IoT sensing devices. *IEEE Internet Things J.* **5**(6), 4589–4597 (2018)
48. A. Yahyaoui, A. Jamil, J. Rasheed, M. Yesiltepe, A decision support system for diabetes prediction using machine learning and deep learning techniques, in *2019 1st International Informatics and Software Engineering Conference (UBMYK)* (2019), pp. 1–4
49. X. Wei, J. Zhao, L. Zhou, Y. Qian, Broad reinforcement learning for supporting fast autonomous IoT. *IEEE Internet Things J.* **7**(8), 7010–7020 (2020)
50. L. Li, A. Ghasemi, IoT-enabled machine learning for an algorithmic spectrum decision process. *IEEE Internet Things J.* **6**(2), 1911–1919 (2019)
51. J. Liao, T. Liu, X. Tang, X. Mu, B. Huang, D. Cao, Decision-making strategy on highway for autonomous vehicles using deep reinforcement learning. *IEEE Access* **8**, 177804–177814 (2020)
52. M. Khalaf, H. Alaskar, A.J. Hussain, T. Baker, Z. Maamar, R. Buyya, P. Liatsis, W. Khan, H. Tawfik, D. Al-Jumeily, IoT-enabled flood severity prediction via ensemble machine learning models. *IEEE Access* **8**, 70375–70386 (2020)
53. K.H. Abdulkareem, M.A. Mohammed, S.S. Gunasekaran, M.N. Al-Mhiqani, A.A. Mutlag, S.A. Mostafa, N.S. Ali, D.A. Ibrahim, A review of fog computing and machine learning: concepts, applications, challenges, and open issues. *IEEE Access* **7**, 153123–153140 (2019)
54. Z.M. Fadlullah, M.M. Fouda, N. Kato, X. Shen, Y. Nozaki, An early warning system against malicious activities for smart grid communications. *IEEE Netw.* **25**(5), 50–55 (2011)
55. M. Ozay, I. Esnaola, F.T. Yarman Vural, S.R. Kulkarni, H.V. Poor, Machine learning methods for attack detection in the smart grid. *IEEE Trans. Neural Netw. Learn. Syst.* **27**(8), 1773–1786 (2016)
56. J. Sakhnini, H. Karimipour, A. Dehghantanha, Smart grid cyber attacks detection using supervised learning and heuristic feature selection, in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)* (2019), pp. 108–112
57. M. Yang, T. Zhu, B. Liu, Y. Xiang, W. Zhou, Machine learning differential privacy with multifunctional aggregation in a fog computing architecture. *IEEE Access* **6**, 17119–17129 (2018)
58. D. Zissis, Intelligent security on the edge of the cloud, in *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (2017), pp. 1066–1070
59. A.L. Buczak, E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **18**(2), 1153–1176 (2016)



# QoS and Energy Efficiency Using Green Cloud Computing



Riman Mandal, Sourav Banerjee, Md Bagbul Islam, Pushpita Chatterjee, and Utpal Biswas

## 1 Introduction

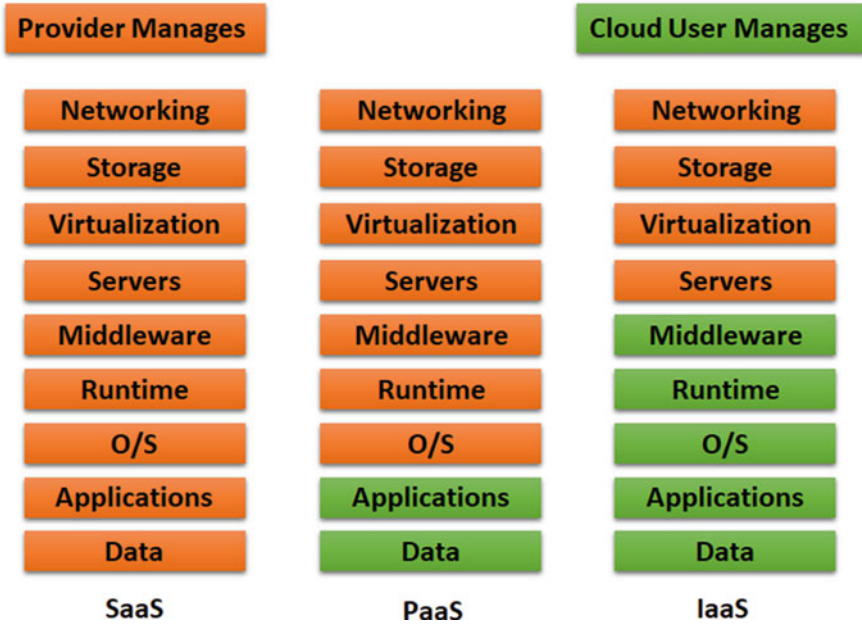
The world has become depended on cloud services due to their flexibilities and dynamic resource-provisioning abilities that comes with minimal pricing. Cloud computing brings computing power and computing environment to cloud users without the installation of costly computers and machine locally. The cloud users can avail different services provided by cloud service providers (CSPs). They need to pay for the services for the time they have utilized the cloud service like a rental system. Different services are provided by different cloud service providers like Amazon Web Service (AWS) [1, 2], Microsoft Azure [2], Google Cloud Platform [3, 4], IBM Cloud, Rackspace, GoDaddy, Verizon Cloud, VMware, and many more all over the globe. These services include infrastructure, platform, software, function, storage, database, security, testing, application, process, integration, and management as a service. Broadly, all cloud services fall under three categories, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), called cloud computing stack because they stacked on top of each other. Figure 1 shows the difference between IaaS, PaaS, and SaaS [5]. On-demand

---

R. Mandal (✉) · U. Biswas  
Department of Computer Science and Engineering, University of Kalyani, Kalyani, West Bengal, India  
e-mail: [utpal01in@ieee.org](mailto:utpal01in@ieee.org)

S. Banerjee · Md. B. Islam  
Department of Computer Science and Engineering, Kalyani Govt. Engineering College, Kalyani, West Bengal, India  
e-mail: [mr.sourav.banerjee@ieee.org](mailto:mr.sourav.banerjee@ieee.org)

P. Chatterjee  
Old Dominion University, Norfolk, VA, USA  
e-mail: [pushpita.c@ieee.org](mailto:pushpita.c@ieee.org)



**Fig. 1** Cloud services: IaaS, PaaS, and SaaS

software applications are provided to cloud users in SaaS. These applications can be accessed from anywhere and any devices. In PaaS, only the data and application need to be managed by the user; the rest of the things are internally handled by the CSP. IaaS provides physical or virtual infrastructures along with networking facilities. A new cloud service model has been developing nowadays called Function-as-a-Service (FaaS). FaaS provides an extra layer abstraction to PaaS. It isolates the users from the background details. FaaS consumes IaaS only when required and hence lowers the pricing of availing FaaS services [5]. To understand the concept of different cloud services, we can take an example of car services. Suppose a car service provider provides three different car services like car lease, car hire, and taxi services. If a car is leased by a customer, then the customer has to bare all the charges for servicing, insurance, fuel, driver, road tolls, etc.; the provider will only provide the car. If a car is rented by a customer, then the customer only has to bare the fuel, toll, and driver charges; the rest of the things will be managed by the car service provider. On a contradictory, if a customer avails a taxi service, the customer only has to pay for the ride. Figure 2 explains car as a service model [5].

These service requests are served by large-scale heterogeneous data centers spread all over the earth. The demand of cloud services is increasing rapidly. To server these colossal service request CSPs build new data centers. These large-scale data centers require continuous power supply to provide uninterrupted services. This electricity is provided by power grids and requires one or more backup power

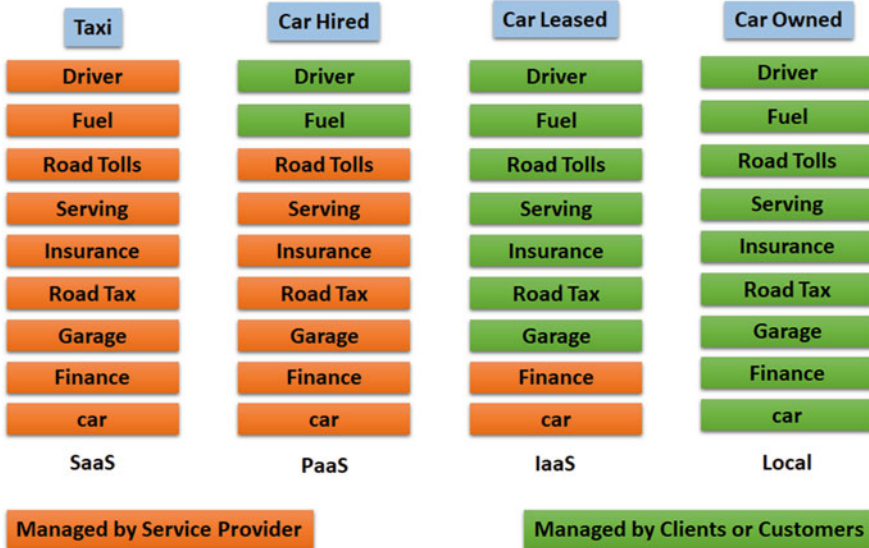


Fig. 2 Car as service

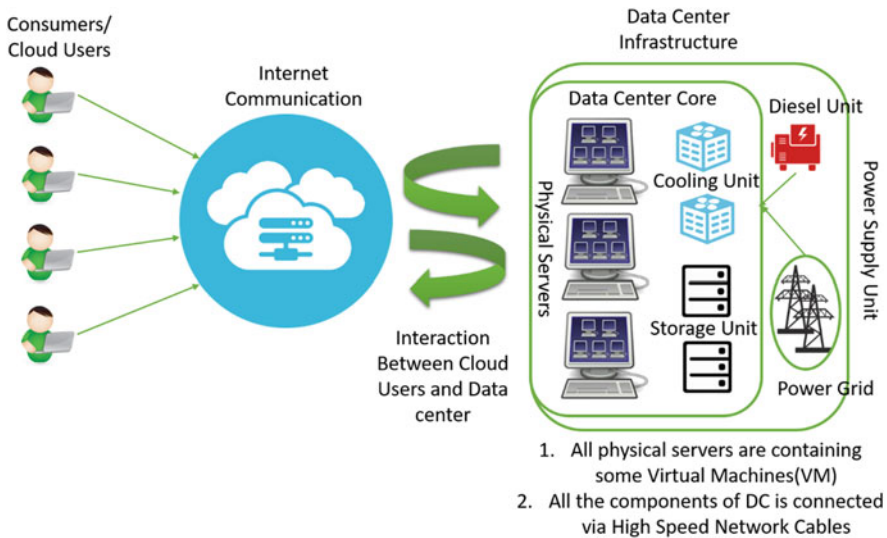


Fig. 3 Cloud data centers

sources in case of grid failures. Figure 3 illustrates cloud computing using data centers [6].

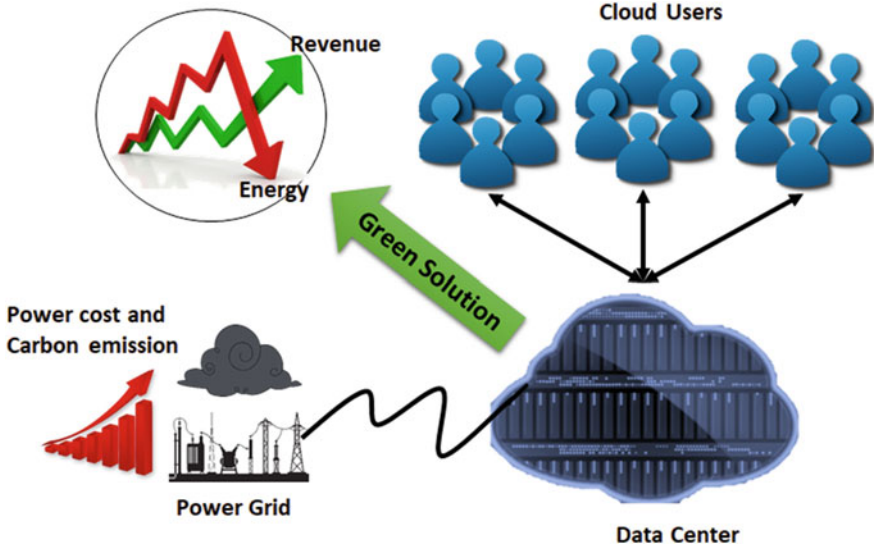
To give an example of the amount of electricity consumed by these data centers, in the year 2017, all the data centers in the world have consumed around 416 terawatts of electricity that is around 3% of the total electricity generated in the

world [7]. The amount of electricity is actually 40% more than all the energy consumed by the UK. Most of these electricities come from fossil fuels that emit a huge amount of greenhouse gases in the environment and increase carbon footprints. According to Pearce [8], data centers emit roughly 900 billion kilogram of CO<sub>2</sub> per year which might be equivalent to the global aviation industry [9].

The users or consumers of these cloud services are increasing very briskly. The CSPs are establishing new data centers to provide stable and uninterrupted service to these growing service requests. With the booming large-scale data centers, electricity requirements are also escalating. These data centers consist of thousands of servers, network devices, racks, and cooling units. On average the cooling units consume almost 45% of the total energy consumed by the data centers. Also idle servers consume more than 50–60% energy consumed by fully utilized servers. Not only the hardware but also inefficient use of computing and network resources along with improper temperature management also adds up to the total energy consumption by the data centers. To tackle the problem of ever-increasing energy consumption, cloud computing needs green solutions.

## 2 Green Cloud Computing

The word “green” with cloud computing ensures that cloud service request will be served in environment-friendly ways [10], that is, to reduce the energy consumption and e-waste from conventional cloud data centers. The energy-efficient use and information technology (IT) and computational resources are known as green computing or green IT [11]. Green cloud computing involves planning, creating, utilizing, and disposing of hardware and software resources of cloud data centers in an environmental sustainable way [10]. But the focus should not be concerned with energy consumption only; rather other factors like operational cost, reliability, timeliness, security, and Quality of Service (QoS) should be maintained. Green cloud computing enables cloud users to avail all the salient features of cloud computing with very less venomous effect on the environment. Figure 4 gives the overview of green cloud computing system [12]. Traditional cloud computing needs a green solution that can help in reducing energy consumption and carbon emission while maintaining the revenue for the CSP. In cloud computing, servers in the data centers are remotely controlled in a virtualized environment. With the emergence of green computing [13], these services can be further enhanced with eco-friendly reusable energy sources which may result in reduced carbon emission. Green cloud computing can increase the energy efficiency of data centers and deliver cost-effective and reliable cloud computing services [14]. Since 2009, researchers are concerned with the energy consumption of data centers and proposed several solutions throughout the years. But some effective and solid solutions are yet to be found. Those researches and knowledge have built the foundation of today’s green cloud computing. In the year 2009, Liu et al. first tossed the term green cloud. They have proposed an architecture based on cloud computing that might help in



**Fig. 4** Green cloud computing overview

reducing the energy consumption by the data centers [15]. An energy-efficient data center called green data center servers is the heart of green cloud computing [16]. In these green data centers, energy consumption will be minimized for all the IT equipment, networking units, and storage units along with every other components of the data centers including building construction, lighting units, cooling units, etc. Also, these green data centers will generate less e-waste, and carbon emission rates will be minimized as much as possible. Designing these green data centers is a difficult job. The design should involve energy-efficient components all over the data center including energy-efficient computing resources or servers, energy-efficient storage units, energy-efficient network equipment, thermal-efficient build design with automatic airflow and heat dissipation, energy-efficient cooling, and lighting equipment. Thermal or heat management is also important because in high temperature, the performance of IT equipment degrades. The servers, storage, and network components all generate heat, and to control the heat, data centers are equipped with cooling units; these cooling units also generate heat to cool down the inside of the building. So, temperature management is extremely important inside and outside of the green data centers to get a sustainable performance.

## 2.1 Applications of Green Cloud Computing

Green cloud applications support all the cloud computing applications with an added feature of environment sustainable computing. Green cloud can be used for creating cloud-based apps and services. It can be used for cloud data storage, backup, and

data recovery system. It can be used by high-definition video and audio platforms like YouTube, Netflix, etc. Online gaming platforms can also use the concepts of green cloud computing. It can be used for delivering on-demand software services. Green cloud computing can be used in efficient processing of big data with very high computational power.

## ***2.2 Advantages of Green Cloud Computing***

There are numerous benefits of using or switching toward green cloud computing which are mainly conserving energy, reduced carbon footprint, reduced e-waste [10], etc.

### **2.2.1 Conserving Electricity**

Through virtualization and resource sharing among users from the world, green cloud computing can save a lot of electricity. According to a survey by Google [10], cloud computing is expected to reduce total energy consumption by 87% for common applications like word processing, spreadsheets, emails, etc. Green data centers are equipped with energy-efficient servers and components. These will reduce the energy consumption drastically.

### **2.2.2 Reduced Carbon Footprint**

With the help of green cloud computing, remote working is possible. People can work from anywhere and anytime in the world. In the COVID-19 pandemic, most of the organizations and private firms are moved toward work from home. They were successful to operate their usual workload from staying at their homes. And some of the organizations want to stay with this kind of working model. Surely the productivity has increased while working from home, and daily commute to the office has drastically reduced. This will save some fossil fuel wasted on daily commutes and reduce carbon footprint in the environment.

### **2.2.3 Going Paperless**

The cloud storage enables paperless system. Files stored in cloud storage can be accessed anytime from anywhere in the world; the user has a minimal Internet service. Papers are created from trees, so trees will be saved if paper usage decreases. Another important aspect is that data stored in these files are stored in a distributed fashion and will not be lost. Data stored in traditional storage system will be lost if the storage system crashes. Papers can be damaged over time and data

might get erased from paper, but files in cloud do not have those limitations. Green cloud computing provides different options to institutions and organizations to move toward paperless transactions. Some well-known green cloud storage systems are Google Drive, OneDrive, Dropbox, etc. which very popular nowadays.

**Secure Transactions** DocuSign and Adobe Sign use green cloud computing technologies to ensure digitally signed secure document verification. They ruled out the possibilities of using printed signed documents. With the help of these green cloud technologies, it is now easier to store, sign, and send contracts, legal documents, and certificates with minimum delay. With the introduction to blockchain technologies, cloud security has already enhanced by twofold.

#### **2.2.4 Reduced e-Waste**

Using shared resources through green cloud computing technologies, e-waste can be reduced drastically. Every year electronic wastes are generated and causing harm to the environment and society. The users do not need to buy intensive computing resources; they can just use cloud shared resources and have their work done from anywhere in the world. This will lead to reduced e-waste and sustainable ecosystem.

#### **2.2.5 Efficient Resource Management**

With the emergence of green computing in the cloud ecosystem, the data center resources can be utilized for better productivity and less operational cost. The green cloud architecture is focused on delivering better QoS to the customers and users while minimizing the energy consumption. Efficient resource management can improve the energy efficiency.

### ***2.3 Shortcoming of Green Cloud Computing***

Though green cloud computing provides lots of benefits to the society and the ecosystem, it has some shortcoming as well.

#### **2.3.1 Implementation Cost**

For small or medium organizations, the deployment cost for green cloud computing will be very high. The system might not be economically feasible to everyone at this moment. But eventually everyone should move toward green technologies for the betterment of the future generation.

### 2.3.2 Evolving Technology

The green cloud computing technology is still new and currently in evolution stage. So it will be difficult to adapt an evolving technology at early states. But surely in the near future, everyone will be able to adapt to the green cloud computing technology.

### 2.3.3 Underpowered Computing

The primary aim of green cloud computing is considered to be the conservation of energy consumption by different computational IT equipment. The applications with high computational requirement might get affected by green cloud computing, as reducing energy consumption of servers might reduce the performance of the servers as well. Green cloud computing has to bring a trade-off between energy consumption and performance to provide better and optimized services.

## 3 Green Computing Approaches

There are mainly two ways that can be acquired by the CSP to improve the energy efficiency: using clean reusable energy as the energy source for the data centers and making the cloud ecosystem energy efficient [16]. And from the cloud users' perspective, replacing old power-hungry system with new and improved low-energy system will do the job. Simple techniques like turning off underutilized servers [17–19] and efficient energy management for the servers can be used to reduce energy consumptions. Going toward more complex techniques like resource management using virtualization [20–27], auto-scaling infrastructure can be used for better energy management [28]. As mentioned earlier, green cloud computing ecosystem is developed on top of green data centers. The architecture of green data centers will ensure maximum environmental sustainability and optimized energy consumption. If all data centers become greener, then it will be a matter of time to implement green cloud computing. Green cloud computing has two different aspects: technical aspects include virtualization, software solutions, hardware improvements, etc. and nontechnical aspects like govt. policies, renewable energy source, cooling, etc.

From the technical perspective, energy-aware hardware techniques and energy-aware software techniques can be used to achieve green cloud computing. Energy-aware techniques may include virtualization [29] techniques like virtual machine (VM) consolidation [30–32] and migration [33, 34], VM scheduling [35, 36], task or job scheduling [37–40], workload consolidation [41, 42], data placement [43], data concentration [44], data replication [45, 46], etc. In hardware techniques energy-efficient IT components [47, 48] like DVFS-enabled CPU, multispeed disks, flash drive, and SSD disks can be used in construction of green data centers.

To minimize the energy consumption of cloud ecosystem, two types of solutions could be applied:



- Minimizing energy consumption of the single server – at server level
- Minimizing energy consumption of the clusters of servers [49] – at data center level

For reducing the energy consumption at server level, several techniques can be applied in different layers such as the application layer, the operational layer, and the compiler layer [49–54]. The solutions [49, 51, 55, 56] could be like:

- Improving the performance of the server per watt.
- CPU clocks could be slowed down, but it might hamper performance.
- Completely turning off unused or underutilized physical servers or equipment.
- Effective workload or task management to get better energy optimization.
- Replacing old components with new ones having better thermal resistance and those able to work on higher-temperature environment.

To reduce the energy consumption at data center level, virtualization techniques could be useful. Virtualization improves reliability, resource management and usage, flexibility, etc. The data center architecture could be optimized for better energy efficiency of the data center. Energy-aware and thermal-aware resource management techniques will contribute to energy saving. Energy-efficient strategies could be employed to use minimal resources for workload processing and putting unused server and data center components to sleep or hibernation [57]. Better thermal management of the data center could improve data centers' performance while maintaining optimized energy consumption. Total energy consumed by data center can be segregated into three different categories: computational energy, networking energy, and energy consumed by the cooling and other hardware units of the data center.

### ***3.1 Dynamic Voltage Frequency Scaling (DVFS)***

DVFS [6] became a standard energy optimization method at hardware levels for cloud and IT industry. It is concerned with adjusting the clock speed according to the load on the system. When load is low, clock speed is slowed down to preserve energy consumption, and when load is high, clock speed is backed up to normal for higher performance. DVFS can be applied to the server cores, DRAMs, and storage units. Mao et al. [58] have proposed a security- and frequency-aware DVFS model that is used to provide security to the cloud applications and improve energy efficiency. They name their system model as SF-DVFS. Hassan et al. [59] have proposed smart energy and reliability-aware scheduling (SERAS) algorithm based on DVFS used for workload scheduling. After analyzing the workload characteristics, SERAS allocates tasks to VMs with modified clock speed achieved using DVFS. SERAS ensures reliability and deadline of the workload as well. They have shown that SERAS achieves 30–50 percentage of energy efficiency over other workload management algorithms. A combinational metaheuristic algorithm has

been proposed by Amulu and Ramraj [60] that uses DVFS technology. They have combined any colony optimization and particle swarm optimization (PSO) to reduce operational cost and time, maintaining the QoS and energy efficiency.

### **3.2 Nano Data Centers (NaDa)**

Traditional data centers consume a huge amount of geographical space and consist of thousands of interconnected servers and computing units. All these components require enormous constant energy source. Nano data centers (NaDa) [61–63] in contradiction use a large number of small energy-efficient data centers working together in a distributed peer-to-peer manner. It has been seen that NaDa are 20–30% more efficient than traditional data centers [64]. As NaDa [65] operates under common authorities, it can achieve better QoS than traditional data centers.

### **3.3 Fast Array of Wimpy Nodes (FAWN)**

FAWN [66, 67] was developed for data-intensive computing. It has an energy-efficient cluster architecture. FAWN is scalable and results in very fast data processing. A large number of “wimpy” nodes are interconnected to form the FAWN clusters. These nodes are built with very fast flash memory coupled with energy-efficient processing cores. This cluster system is able to achieve the same level of performance like traditional data centers but uses a fraction of the energy.

### **3.4 Virtualization and VM Consolidation**

Efficient resource sharing using server virtualization helps in reducing energy consumption. Figure 5 illustrates cloud architecture with virtualization and consolidation. The cloud users submit service request to the global resource manager (GRM). A service-level agreement (SLA) is established between CSP and cloud users that ensures QoS. GRM uses different task allocation policies to allocate users’ task to different VMs running on physical servers in the data center. Periodically, the servers are analyzed for underutilized server detection, and the VMs from those servers are migrated to other moderate loaded servers. Then underutilized servers are turned off to conserve electricity.

Beloglazov and Buyya [68] have proposed a virtualization and VM consolidation framework that is currently widely used. They have proposed a cloud architecture where workloads are allotted to different VMs by analyzing the workload requirements. These VMs are then placed in physical servers using VM allocation policies. Later, through overload and underload detection algorithms, servers are

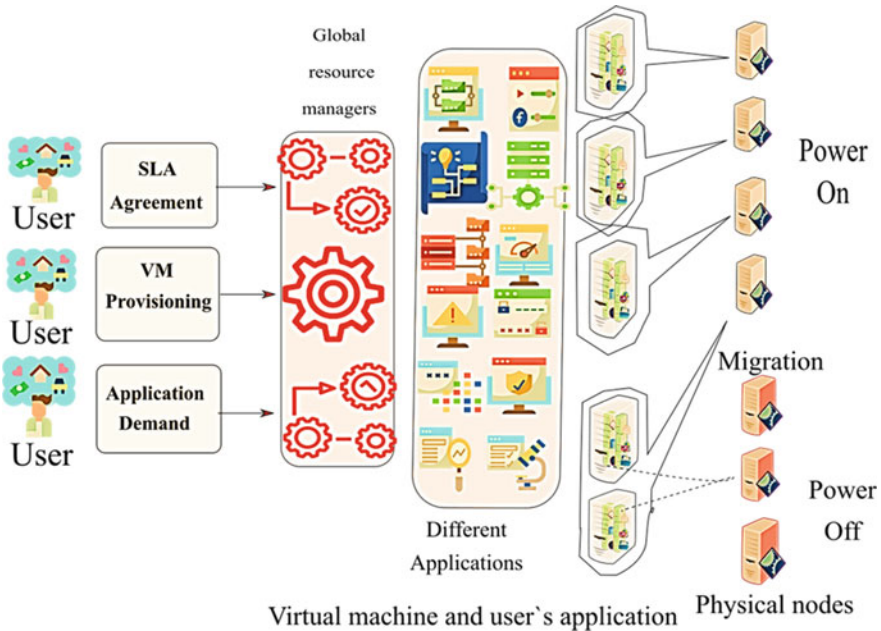


Fig. 5 Virtualized cloud ecosystem

classified into three categories: overloaded, underutilized, and moderate loaded servers. Overloaded servers tend to violate the SLA agreement, so some load needs to shift to moderate loaded servers. VM selection policies are used to identify which VM needs migration to new servers. Underutilized servers are put to sleep after migrating all the VMs to moderate loaded servers to minimize energy consumed by those servers. This process is repeated after a certain period of time. They have proposed power-aware VM allocation policy and claimed to have better energy efficiency than traditional cloud architecture.

Li et al. [69] analyzed that VM consolidation is a critical task, and a non-optimized VM placement may lead to repeated VM migrations leading to aggregation in energy consumption and performance degradation. They have proposed EQ-VMC algorithm to optimize VM consolidation with the help of a discrete differential evolution algorithm that searches for global optimal solution. Haghshenas and Mohammadi [70] have used regression-based dynamic VM consolidation approach to predict the resource requirement of a workload allocated to a VM. They claimed to have achieved 39% energy efficiency over conservative VM consolidation algorithms. Their approach was more scalable and 5% faster as well. Mandal et al. [29] have proposed a VM selection policy that selects the VM having the highest utilization for migration. They have successfully able to reduce the energy consumption while maintaining decent SLA violation.

### ***3.5 Geographical Location and Data Center Cooling***

The geographical location of data center can be an important factor for reducing energy consumption. Data centers can be built in a location having cold atmosphere that will help to reduce energy consumption by the cooling units. Data centers near renewable energy source could be beneficial for CSP as well as environment. Energy cost will be reduced and carbon footprint will be minimized with the use of renewable energy. Microsoft and Google have recently moved into the use of clean energy for their data centers.

Cooling units of data centers consume a lot of electricity. Data centers should be equipped with air cooling system. Microsoft has implanted an air-cooled data center in Ireland. This data center requires 60% less electricity than other data centers. The conventional cooling systems generate heat well. The cooling systems should be upgraded with heat absorption cooling that is environment friendly. This type of cooling systems is known as Organic Rankine Cycle (ORC). ORC is considered to be an efficient cooling technology for data centers.

## **4 Security in Green Cloud Computing**

Though green cloud computing provides several environment sustainable benefits to the CSP and cloud user, often consumers hesitate to move toward cloud infrastructure and services as they believe data in cloud are not secure. Data hosted in public cloud setup might get lost or lacked that business industries are also concerned. Different cybersecurity threats in green cloud ecosystem are listed below.

### ***4.1 Consumer Apprehensions Toward Green Cloud Security***

#### **4.1.1 Loss or Theft of Intellectual Property**

When moving to the cloud, users also fear the loss or misuse of intellectual property (IP). In 2018, over 3.3 million patent applications were filed. The IPs demonstrate the economic benefits of the holding firms. IP failure or theft can cause considerable harm to the parent business, as goods can also be imitated by many other companies in the same sector [71].

#### **4.1.2 Regulatory Compliance Violations**

A specific compliance guideline is defined by every business firm for their field of business. When moving toward green cloud computing services, the CSP must

ensure to follow these compliances. When CSP fails to adhere these guidelines, compliance-related security breaches might happen [71].

### **4.1.3 Minimal Visibility of the Cloud Ecosystem**

Another key concern for the business and firm that CSP does not provide is any clear visibility of the cloud infrastructure. Though if consumers opt for IaaS- or PaaS-based green cloud services, they somehow get the flexibility to configure their own green cloud ecosystem.

### **4.1.4 Less Control**

Like visibility, CSP provides very little control to its customers. Most of the cloud environment settings are controlled by CSP itself. Consumers may not like these activities.

### **4.1.5 Lateral Spreading of Attacks**

If green cloud computing could not provide sufficient security measures, it might be easier for cyberattacks to breach the security of distributed file system and attack one resource after another. This can result in lateral spreading of attacks. It will compromise several databases at once.

## ***4.2 Green Cloud Security Aspects***

It has been seen that most of the cloud cyberattacks and data breaches in cloud infrastructure are caused by consumer error and misconfiguration vulnerabilities. Business should follow some basic practices to ensure green cloud security.

### **4.2.1 Access Control and Least Privilege**

Strong user access control systems must be defined by the business admins to determine who can and to what extent can access the data. Limited access will ensure that only authorized personnel have access to cloud data. In addition, the implementation of the least privilege model guarantees that only approved users can access the data they need to complete their proper tasks.

#### 4.2.2 Using SSH and Securely Store Keys

One can create stable server connections with private and public key pairs with the aid of Secure Socket Shell (SSH) keys. Since these keys are used to access sensitive data and perform critical tasks, it is imperative for companies to maintain and store these SSH keys safely. Business firms should implement different policies related to green cloud computing for monitoring these keys.

#### 4.2.3 Using Encryption in Cloud

All green cloud system should implement encryption technologies to move in and out that cloud data. Today, almost all CSPs provide different encryption services. CSPs should have the knowledge of the security needs of the customers and ensure those security features.

#### 4.2.4 Routing Penetration Tests

Security vulnerabilities present in cloud system can be identified by performing cloud routing penetration tests. Penetration tests can be performed by both the parties involved in cloud transactions.

#### 4.2.5 Multi-Factor Authentication (MFA)

MFA means using several authentication methods like biometrics, OTP, questionnaire, etc. applied altogether. Companies or firms can use MFA to secure cloud data and accounts. MFA can ensure only authorized personnel can access the data and protects the data from stolen or compromised login credentials.

Li et al. [23] have developed CyberGuarder which is a virtualization security assurance tool used for green cloud computing. It was designed to identify and resolve several security issues within green cloud computing. CyberGuarder provided a virtual machine manager (VMM)-based integrity solution for trusted loading of network software applications (NetApp). It also has the feature of NetApp isolation to ensure user isolation. They have also incorporated a trust management system. Gill and Sharma [72] have analyzed that to provide green cloud security, different security appliances are used. These appliances require energy consumption that adds up to the total energy consumption of the cloud ecosystem. They have developed Intrusion Detection and Prevention System (IDPS) to ensure security in virtual network. They have implemented the prototype that did its intended job. Torkura et al. [73] have implemented Risk-Driven Fault Injection (RDFI) techniques to address the security issues of green cloud computing. With the help of chaos engineering, RDFI is able to monitor, analyze, execute, and plan security fault

injection campaigns. They used a knowledge base that consists of different fault models.

## 5 Conclusion

In this chapter, a critical analysis of green cloud computing was done based on energy consumption and security aspects of green cloud. Green computing is not a new concept; GoingGreen was introduced in 1992. The green cloud computing architecture was developed to deploy cost-efficient cloud services with minimal or no effect on environment. Green cloud can provide real-time performance ensuring QoS to the customers. Several advantages and disadvantages of green cloud were discussed throughout the chapter. Despite all the shortcomings, these technology needs development for the betterment of our ecosystem. This cloud paradigm is in developing stage and needs more improvements in the near future. The security issues need to be analyzed in more details. Security issues in green cloud computing can be resolved with the joint effort of CSP and customers. Misusing the information stored in cloud environment can lead to several problems; the security measures need more attention from the researchers.

## References

1. S. Mathew, J. Varia, Overview of Amazon Web Services, Amaz. Whitepapers (2014)
2. C. Kotas, T. Naughton, N. Imam, A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing, in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–4
3. S. Challita, F. Zalila, C. Gourdin, P. Merle, A precise model for google cloud platform, in *2018 IEEE International Conference on Cloud Engineering (IC2E)*, 2018, pp. 177–183
4. X. Jia, Google cloud computing platform technology architecture and the impact of its cost, in *2010 Second World Congress on Software Engineering*, 2010, vol. 2, pp. 17–20
5. S. Kale, Cloud Computing – Types of Cloud, *ESDS*, Jan. 18, 2021. <https://www.esds.co.in/blog/cloud-computing-types-cloud/#sthash.yymu3L0e.dpbs> (accessed Feb. 01, 2021)
6. R. Mandal, M.K. Mondal, S. Banerjee, C. Chakraborty, U. Biswas, A survey and critical analysis on energy generation from datacenter, in *Data Deduplication Approaches*, (Elsevier, 2021), pp. 203–230
7. A. Marashi, Improving Data Center Power Consumption & Energy Efficiency, *VXCH-NGE*, Feb. 12, 2020. <https://www.vxchnge.com/blog/growing-energy-demands-of-data-centers> (accessed Feb. 02, 2020)
8. F. Pearce, Energy Hogs: Can World’s Huge Data Centers Be Made More Efficient?, *YaleEnvironment360*, Apr. 03, 2018. <https://e360.yale.edu/features/energy-hogs-can-huge-data-centers-be-made-more-efficient> (accessed Apr. 02, 2020)
9. Facts and Figures, *Air Transport Action Group*, Sep. 2020. <https://www.atag.org/facts-figures.html> (accessed Feb. 02, 2020)
10. A. Ohri, Green Cloud Computing: A Beginner’s Guide, *Jigsaw Academy*, Nov. 23, 2020. <https://www.jigsawacademy.com/blogs/cloud-computing/green-cloud-computing/> (accessed Jan. 02, 2021)

11. Y. Mathur, Green Cloud Computing, *Lucid Outstanding Solutions*, Sep. 22, 2018. <https://lucidoutsourcing.com/blog/green-cloud-computing> (accessed May 02, 2021)
12. S.K. Garg, R. Buyya, Green cloud computing and environmental sustainability. *Harnessing Green IT Princ. Pract.* **2012**, 315–340 (2012)
13. J. Liu, F. Zhao, X. Liu, W. He, Challenges towards elastic power management in internet data centers, in *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, 2009, pp. 65–72
14. Y. S. Patel, N. Mehrotra, S. Soner, Green cloud computing: A review on Green IT areas for cloud computing environment, in *2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, 2015, pp. 327–332
15. L. Liu et al., GreenCloud: a new architecture for green data center, in *Proceedings of the 6th international conference industry session on Autonomic computing and communications industry session*, 2009, pp. 29–38
16. L.-D. Radu, Green cloud computing: A literature survey. *Symmetry* **9**(12), 295 (2017)
17. N. Xiong, W. Han, A. Vandenberg, Green cloud computing schemes based on networks: A survey. *IET Commun.* **6**(18), 3294–3300 (2012)
18. B. Wadhwa, A. Verma, Energy and carbon efficient VM placement and migration technique for green cloud datacenters, in *2014 Seventh international conference on contemporary computing (IC3)*, 2014, pp. 189–193
19. B. Wadhwa, A. Verma, Energy saving approaches for Green Cloud Computing: A review, in *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, 2014, pp. 1–6
20. N. Sabry, P. Krause, Optimal green virtual machine migration model. *Int. J. Bus. Data Commun. Netw. IJBDCN* **9**(3), 35–52 (2013)
21. Q. Chen, P. Grosso, K. van der Veldt, C. de Laat, R. Hofman, H. Bal, Profiling energy consumption of VMs for green cloud computing, in *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, 2011, pp. 768–775
22. G. B. Fioccola, P. Donadio, R. Canonico, G. Ventre, Dynamic routing and virtual machine consolidation in green clouds, in *2016 IEEE international conference on cloud computing technology and science (CloudCom)*, 2016, pp. 590–595
23. J. Li et al., CyberGuarder: A virtualization security assurance architecture for green cloud computing. *Futur. Gener. Comput. Syst.* **28**(2), 379–390 (2012)
24. S.K. Mishra et al., Energy-efficient VM-placement in cloud data center. *Sustain. Comput. Inform. Syst.* **20**, 48–55 (2018)
25. A. Khosravi, S. K. Garg, R. Buyya, Energy and carbon-efficient placement of virtual machines in distributed cloud data centers, in *European Conference on Parallel Processing*, 2013, pp. 317–328
26. W. Wei, H. Gu, W. Lu, T. Zhou, X. Liu, Energy efficient virtual machine placement with an improved ant colony optimization over data center networks. *IEEE Access* **7**, 60617–60625 (2019)
27. B. Kar, E.H.-K. Wu, Y.-D. Lin, Energy cost optimization in dynamic placement of virtualized network function chains. *IEEE Trans. Netw. Serv. Manag.* **15**(1), 372–386 (2017)
28. B. Dougherty, J. White, D.C. Schmidt, Model-driven auto-scaling of green cloud computing infrastructure. *Futur. Gener. Comput. Syst.* **28**(2), 371–378 (2012)
29. R. Mandal, M.K. Mondal, S. Banerjee, U. Biswas, An approach toward design and development of an energy-aware VM selection policy with improved SLA violation in the domain of green cloud computing. *J. Supercomput.* **76**(9), 7374–7393 (Sep. 2020). <https://doi.org/10.1007/s11227-020-03165-6>
30. F. Farahnakian et al., Energy-aware dynamic VM consolidation in cloud data centers using ant colony system, in *2014 IEEE 7th International Conference on Cloud Computing*, 2014, pp. 104–111
31. D.-K. Kang, F. Alhazemi, S.-H. Kim, C.-H. Youn, Dynamic virtual machine consolidation for energy efficient cloud data centers, in *International Conference on Cloud Computing*, 2015, pp. 70–80



32. N.K. Biswas, S. Banerjee, U. Biswas, U. Ghosh, An approach towards development of new linear regression prediction model for reduced energy consumption and SLA violation in the domain of green cloud computing. *Sustain. Energy Technol. Assess.* **45**, 101087 (2021)
33. M. H. Al Shayeji, M. Samrajesh, An energy-aware virtual machine migration algorithm, in *2012 International Conference on Advances in Computing and Communications*, 2012, pp. 242–246
34. V. R. Reguri, S. Kogatam, M. Moh, Energy efficient traffic-aware virtual machine migration in green cloud data centers, in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 2016, pp. 268–273
35. S. Banerjee, R. Mandal, U. Biswas, An approach towards amelioration of an efficient VM allocation policy in cloud computing domain. *Wirel. Pers. Commun.* **98**(2), 1799–1820 (Jan. 2018). <https://doi.org/10.1007/s11277-017-4946-0>
36. L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, X. Xu, A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. *World Wide Web* **23**(2), 1275–1297 (2020)
37. S. Banerjee, A. Roy, A. Chowdhury, R. Mutsuddy, R. Mandal, U. Biswas, An approach toward amelioration of a new clouddlet allocation strategy using Cloudsim. *Arab. J. Sci. Eng.* **43**(2), 879–902 (Feb. 2018). <https://doi.org/10.1007/s13369-017-2781-y>
38. Q. Tang, S.K.S. Gupta, G. Varsamopoulos, Energy-efficient thermal-aware task scheduling for homogeneous high-performance computing data centers: A cyber-physical approach. *IEEE Trans. Parallel Distrib. Syst.* **19**(11), 1458–1472 (2008). <https://doi.org/10.1109/TPDS.2008.111>
39. T. V. T. Duy, Y. Sato, and Y. Inoguchi, Performance evaluation of a Green Scheduling Algorithm for energy savings in Cloud computing, in *2010 IEEE International Symposium on Parallel Distributed Processing, Workshops and Phd Forum (IPDPSW)*, 2010, pp. 1–8, doi: <https://doi.org/10.1109/IPDPSW.2010.5470908>
40. H. Chen, X. Zhu, H. Guo, J. Zhu, X. Qin, J. Wu, Towards energy-efficient scheduling for real-time tasks under uncertain cloud computing environment. *J. Syst. Softw.* **99**, 20–35 (2015)
41. S. Srikantaiah, A. Kansal, and F. Zhao, Energy Aware Consolidation for Cloud Computing, Dec. 2008, USENIX HotPower'08: Workshop on Power Aware Computing and Systems at OSDI., [Online]. Available: <https://www.microsoft.com/en-us/research/publication/energy-aware-consolidation-for-cloud-computing/>
42. G. Prekas, M. Primorac, A. Belay, C. Kozyrakis, E. Bugnion, Energy proportionality and workload consolidation for latency-critical applications, in *Proceedings of the Sixth ACM Symposium on Cloud Computing*, Kohala Coast Hawaii, Aug. 2015, pp. 342–355, doi: <https://doi.org/10.1145/2806777.2806848>
43. R. Reddy, A. Kathpal, J. Basak, R. Katz, Data layout for power efficient archival storage systems, in *Proceedings of the Workshop on Power-Aware Computing and Systems*, 2015, pp. 16–20
44. D. K. Lee, K. Koh, PDC-NH: Popular data concentration on NAND flash and hard disk drive, in *2009 10th IEEE/ACM International Conference on Grid Computing*, 2009, pp. 196–200, doi: <https://doi.org/10.1109/GRID.2009.5353061>
45. S. Iwata, K. Shiozawa, A simulation result of replicating data with another layout for reducing media exchange of cold storage, (2016)
46. N. Zhao, J. Wan, J. Wang, C. Xie, GreenCHT: A power-proportional replication scheme for consistent hashing based key value storage systems, in *2015 31st Symposium on Mass Storage Systems and Technologies (MSST)*, 2015, pp. 1–6
47. A. Shafiee, et al., ISAAC: A Convolutional Neural Network Accelerator with In-Situ Analog Arithmetic in Crossbars, in *2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)*, 2016, pp. 14–26, <https://doi.org/10.1109/ISCA.2016.12>
48. M. M. Ozdal, et al., Energy Efficient Architecture for Graph Analytics Accelerators, in *2016 ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)*, 2016, pp. 166–177, <https://doi.org/10.1109/ISCA.2016.24>

49. W. Itani, C. Ghali, A. Kayssi, A. Chehab, I. Elhajj, G-route: An energy-aware service routing protocol for green cloud computing. *Clust. Comput.* **18**(2), 889–908 (Jun. 2015). <https://doi.org/10.1007/s10586-015-0443-y>
50. S.K. Garg, C.S. Yeo, A. Anandasivam, R. Buyya, Environment-conscious scheduling of HPC applications on distributed Cloud-oriented data centers. *J. Parallel Distrib. Comput.* **71**(6), 732–749 (Jun. 2011). <https://doi.org/10.1016/j.jpdc.2010.04.004>
51. S.-Y. Jing, S. Ali, K. She, Y. Zhong, State-of-the-art research study for green cloud computing. *J. Supercomput.* **65**(1), 445–468 (Jul. 2013). <https://doi.org/10.1007/s11227-011-0722-1>
52. S. P. Reddy, H. K. S. Chandan, Energy aware scheduling of real-time and non real-time tasks on cloud processors (Green Cloud Computing), in *International Conference on Information Communication and Embedded Systems (ICICES2014)*, 2014, pp. 1–5, <https://doi.org/10.1109/ICICES.2014.7033827>
53. J. Conejero, O. Rana, P. Burnap, J. Morgan, B. Caminero, C. Carrión, Analyzing Hadoop power consumption and impact on application QoS. *Futur. Gener. Comput. Syst.* **55**, 213–223 (Feb. 2016). <https://doi.org/10.1016/j.future.2015.03.009>
54. C. Cappiello, N.T.T. Ho, B. Pernici, P. Plebani, M. Vitali, CO<sub>2</sub>-aware adaptation strategies for cloud applications. *IEEE Trans. Cloud Comput.* **4**(2), 152–165 (Apr. 2016). <https://doi.org/10.1109/TCC.2015.2464796>
55. S. R. Hussein, Y. Alkabani, H. K. Mohamed, Green cloud computing: Datacenters power management policies and algorithms, in *2014 9th International Conference on Computer Engineering Systems (ICCES)*, 2014, pp. 421–426, <https://doi.org/10.1109/ICCES.2014.7030998>
56. L. A. Rocha, E. Cardozo, A Hybrid Optimization Model for Green Cloud Computing, in *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, 2014, pp. 11–20, <https://doi.org/10.1109/UCC.2014.9>
57. D. Kliazovich, P. Bouvry, S.U. Khan, GreenCloud: A packet-level simulator of energy-aware cloud computing data centers. *J. Supercomput.* **62**(3), 1263–1283 (Dec. 2012). <https://doi.org/10.1007/s11227-010-0504-1>
58. J. Mao, T. Cao, X. Peng, T. Bhattacharya, W.-S. Ku, and X. Qin, “Security-Aware Energy Management in Clouds,” in *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2020, pp. 284–293, <https://doi.org/10.1109/TPS-ISA50397.2020.00044>
59. H.A. Hassan, S.A. Salem, E.M. Saad, A smart energy and reliability aware scheduling algorithm for workflow execution in DVFS-enabled cloud environment. *Futur. Gener. Comput. Syst.* **112**, 431–448 (Nov. 2020). <https://doi.org/10.1016/j.future.2020.05.040>
60. L.M. Amulu, R. Ramraj, Combinatorial meta-heuristics approaches for DVFS-enabled green clouds. *J. Supercomput.* **76**(8), 5825–5834 (Aug. 2020). <https://doi.org/10.1007/s11227-019-02997-1>
61. J. He, A. Chaintreau, C. Diot, A performance evaluation of scalable live video streaming with nano data centers. *Comput. Netw.* **53**(2), 153–167 (Feb. 2009). <https://doi.org/10.1016/j.comnet.2008.10.014>
62. N. Laoutaris, P. Rodriguez, L. Massoulié, ECHOS: Edge capacity hosting overlays of nano data centers. *ACM SIGCOMM Comput. Commun. Rev.* **38**(1), 51–54 (Jan. 2008). <https://doi.org/10.1145/1341431.1341442>
63. V. Valancius, N. Laoutaris, L. Massoulié, C. Diot, P. Rodriguez, Greening the internet with nano data centers, in *Proceedings of the 5th international conference on Emerging networking experiments and technologies - CoNEXT '09*, Rome, Italy, 2009, p. 37, <https://doi.org/10.1145/1658939.1658944>
64. A.D. Borah, D. Muchahary, S.K. Singh, J. Borah, Power saving strategies in green cloud computing systems. *Int. J. Grid Distrib. Comput* **8**(1), 299–306 (Feb. 2015). <https://doi.org/10.14257/ijgcd.2015.8.1.28>
65. K. Kaur, T. Dhand, N. Kumar, S. Zeadally, Container-as-a-service at the edge: Trade-off between energy efficiency and service availability at Fog Nano Data Centers. *IEEE Wirel. Commun.* **24**(3), 48–56 (2017). <https://doi.org/10.1109/MWC.2017.1600427>

66. D. G. Andersen, J. Franklin, M. Kaminsky, A. Phanishayee, L. Tan, V. Vasudevan, FAWN: A fast array of wimpy nodes, in *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*, 2009, pp. 1–14
67. L.A. Barroso, FAWN: A fast array of wimpy nodes: Technical perspective. *Commun. ACM* **54**(7), 100–100 (Jul. 2011). <https://doi.org/10.1145/1965724.1965746>
68. A. Beloglazov, R. Buyya, Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers. *Concurr. Comput. Pract. Exp.* **24**(13), 1397–1420 (2012)
69. Z. Li, X. Yu, L. Yu, S. Guo, V. Chang, Energy-efficient and quality-aware VM consolidation method. *Futur. Gener. Comput. Syst.* **102**, 789–809 (Jan. 2020). <https://doi.org/10.1016/j.future.2019.08.004>
70. K. Haghshenas, S. Mohammadi, Prediction-based underutilized and destination host selection approaches for energy-efficient dynamic VM consolidation in data centers. *J. Supercomput.* **76**(12), 10240–10257 (Dec. 2020). <https://doi.org/10.1007/s11227-020-03248-4>
71. R. Sinha, Cybersecurity in The Cloud: Here's What It Means, *ESDS*, Jul. 21, 2020. <https://www.esds.co.in/blog/cybersecurity-in-the-cloud-heres-what-it-means/#sthash.lom6AXHa.dpbs> (accessed Oct. 02, 2021)
72. K. S. Gill, A. Sharma, IDPS based framework for security in green cloud computing and comprehensive review on existing frameworks and security issues, in *2015 International Conference on Computing, Communication and Security (ICCCS)*, 2015, pp. 1–6, <https://doi.org/10.1109/CCCS.2015.7374153>
73. K.A. Torkura, M.I.H. Sukmana, F. Cheng, C. Meinel, CloudStrike: Chaos engineering for security and resiliency in cloud infrastructure. *IEEE Access* **8**, 123044–123060 (2020). <https://doi.org/10.1109/ACCESS.2020.3007338>

# Privacy Issues in Smart IoT for Healthcare and Industry



Kateryna Mokliakova and Gautam Srivastava 

## 1 Introduction

The concept of IoT is not new; however, the real “boom” of technology has happened through the past 10 years and continues to grow. Because of the endless potential of IoT in medicine, transport, security, and home facilities, smart devices are our future. In addition, IHS Markit [1] forecasts nonlinear growing of IoT number to 125 billion devices by 2030. Eventually, massiveness of IoT devices is one of the reasons why we need to speak about their security and why it is important. IoT are used in several areas to automate peoples’ work and make their life easier. Such areas are manufacturing, transportation, home automation, etc. While these areas are focused to reduce human interaction and provide a machine-to-machine model, the critical aspect of managing smart devices in healthcare remains.

One of the main benefits of using the Internet of Things in healthcare is data monitoring in real time and quick response that improves predictions and precautions for patients’ health. The primary Internet of Things architecture implies easy remote configuration and control through wireless access to primary devices. Despite the comfortable usage of such technologies, the security risks must be accepted. Trends around intelligent IoT provide involvement of security researches that gives a better understanding and awareness of security issues.

The role of IoT in medicine lays in several areas according to [1]; they are:

- Eldercare: this area includes looking after elderly residents or patients at nursing homes or hospitals.

---

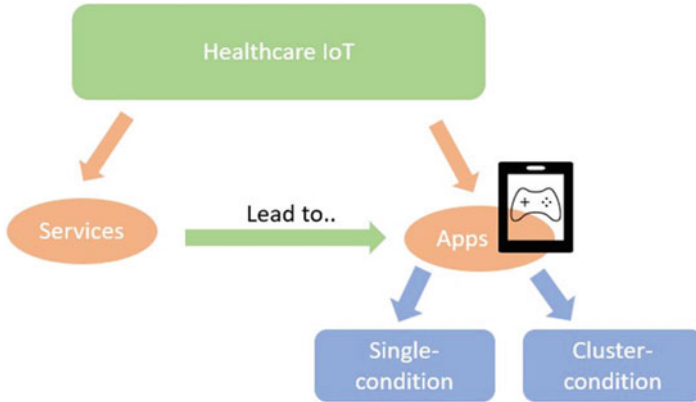
K. Mokliakova

Faculty of Information Technology, National Taras Shevchenko University of Kyiv, Kyiv, Ukraine

G. Srivastava (✉)

Department of Math and Computer Science, Brandon University, Brandon, MB, Canada

e-mail: [srivastavag@brandonu.ca](mailto:srivastavag@brandonu.ca)



**Fig. 1** Healthcare IoT building

- Gathering of data is the most grown-up area in healthcare; it involves much equipment that we see at the bedside in hospitals like the EKG monitor; this area continues to expand with innovations happening in the world of IoT.
- Real-time location is used to track people and assets without additional cost.

Analysis of the data collected via digital medical records, diagnostic information gathered through imaging devices, and portable personal computers or tablets will enrich the decision-making powers. This will give patients more opportunities to manage their health.

It is common to see IoT devices in patients' rooms, electronic medical records, and other cloud-based resources in hospitals. Connecting new devices is an ongoing initiative at most healthcare organizations. But, on the other hand, the challenge of interoperability of devices occurs, which can lead to either new security vulnerabilities and additional risks or network exposure.

According to the US National Security Telecommunications Advisory Committee (NSTAC), IoT can be divided into three fundamentals, which are devices, platforms, and intelligence [2]. A quick overview of how IoT in healthcare works is simply shown by "The Internet of Things for Health Care: A Comprehensive Survey Article" [3]. According to this study, the healthcare IoT can be categorized as applications and services. Applications are further divided into two groups: single- and clustered-condition applications. A single-condition application refers to a specific disease or infirmity, while a clustered-condition application deals with several diseases or conditions together as a whole. Healthcare aspects are shown in Fig. 1. Requests are redirected by the required services.

Healthcare services in the scope of industrial IoT (IIoT) – smart connected assets (the things) that operate as part of a larger system or systems of systems that make up the smart manufacturing enterprise [4] – are a subset of different problem solutions made from applications and technologies.

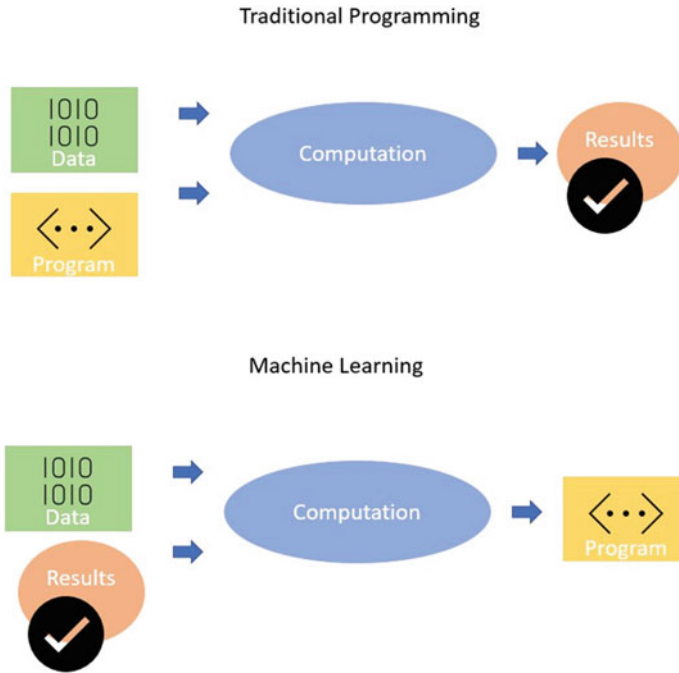


Fig. 2 Machine learning vs. traditional programming approach

Trends toward the healthcare IIoT tech base are described in “Trends in IoT based solutions for health care: Moving AI to the edge” [5]. IoT solutions are evolving from simple architectures to more complex with a purpose to collect, transmit, and visualize data acquired by field and wearable sensor networks to complex smart systems that are able to provide analytics, recognize activities, and make decisions. So, artificial intelligence and machine learning followed by their needs in cloud services and big data are the main trends in smart devices technologies. IoT and machine learning are powerful tools that provide advanced service [6]. The key point of machine learning is its difference from traditional programming: while programming takes *data* and *program* to provide a *result*, machine learning operates with data and results to produce a program (Fig. 2).

For example, you are an employee at the supermarket where smart IoT cameras are installed. Suddenly, the man with a mask and gun has come to rob you. The camera takes the data: a man in a mask holding a gun; as a result – the employee is in danger, and run a program – call 911. Smart IoT here represents that the IoT possesses self-abilities or capabilities such as self-learning, self-adapting, and self-reasoning to adapt to dynamic environments.

Machine learning in pharma and medicine is a future where data, analysis, and innovation work together to help countless patients without interaction with them. Crowdsourced data collection with IoT has big potential in the healthcare industry.

The subject of obtaining information from a large and relative to the topic group of people is in all trends in medicine nowadays. Researchers and practitioners then have access to a large amount of reference uploaded by people with their permission. A large amount of crowdsourced data can be collected by IoT devices, processed in the cloud environment, and sent back to provide high-quality service. It is known for a fact that smart devices improve. Besides, medicine also comes across new ways of using the data: work on tough-to-diagnose samples and help in the general improvement of diagnosis and treatment. For more information about ML-based application in healthcare, see [7].

Also, according to the Case Study of Authorization Model for IoT Healthcare Systems, many approaches using blockchain, fog computing, edge computing, and machine learning have been proposed to solve security issues [8].

Blockchain is a secure mechanism proposed in 1991 [9]. Simply, the principle of its operation is storing the operations/transactions sequentially; these operations/transactions represented using Merkle tree [5]. Each operation/transaction has a cryptography hash code, and it is stored in the tree leaf node. Every two contiguous leaf nodes are concatenated, and a new root hash is generated until the final root hash created and it is stored on the blockchain. The root hash can be confirmed to ensure that all the exchanges related to that root hash are secure and have not been changed. In case a single operation/transaction is changed, all the hash values on that particular side of the tree will change [8]. Other technologies proposed are fog and edge computing. These technologies utilize IoT devices as a lower layer. As examples, we can see many smart actuators, sensors, cameras, cards, and smartphones. Adding to that are personal medical monitor, home, and business artificial intelligence (AI) devices, etc.

Security problems mainly lay in a little attention to security in the projecting and implementing process, because new productions must be faster and faster to fulfill customers' expectations and needs. This means healthcare IoT is "easy to hack and hard to patch" as mentioned in [10]. Application risks, such as breaches of authentication and authorization, as well as the overall security and availability of the applications are also considered as a concern [11]. The easy access to the devices physically from within the network or remotely and inherent vulnerabilities as weak passwords often the default ones, no built-in security, outdated and legacy firmware or software – like managed computers running old or not updated vulnerable versions of Windows, etc. – are the first indicators that such devices need to be protected and used with carefulness.

## 2 Related Works

For several years a great effort has been devoted to the study of IoT privacy and security [11, 12, 18, 30, 32, 33, 35]. Plenty of researches for accurate solutions were conducted in healthcare IoT [1, 15, 23]; also they include secure network protocol for subscribing/publishing IoT architecture [8], a privacy-enhancing framework

[14], authorization model for healthcare systems [36], privacy and security measures in IoT [37], etc. However, hackers also are aware of poor IoT security, and new attacks are reported either from healthcare organizations or other sectors [13, 20–22].

It is also important to remember about the specific of healthcare IoT devices that are organized in works [3, 7]. Some basic definitions are held by [17, 19, 29, 31].

As technology moves forward, new trends occur in the IoT area as well. In [4–6], the authors describe the most recent movements in IoT involving blockchain technology machine learning, and cloud computing.

Besides, best practices and principles of IoT device protection were determined in Ref. [2, 10, 27, 34]. Some guidelines of secure usage of IoT devices in the industry were developed by public organizations like NIST [16, 24, 28], ENISA [25], and GSMA [26]. Those studies consist of recommendations and standards about stressless implementation and secure operation of the set of IoT devices in healthcare.

### 3 Privacy Issues in Healthcare IoT

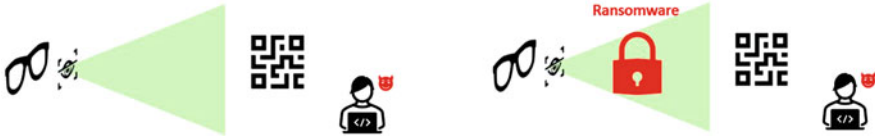
Surveys about poor security around IoT have started since the first devices were sold. However, it does not affect much. As we can look through researches from 2008 to 2019 [12], the same issues stay across. Numerous works are pointed to privacy issues in IoT and healthcare. Studies of security difficulties and vulnerabilities in the IoT area continue nowadays. M. Conti, A. Dehghantanha, K. Franke, and S. Watson [13] discussed two kinds of difficulties in the IoT environment that are security and forensics challenges.

Cybersecurity in healthcare is a property of a well-designed system. During the planning process, the inventors should think about the vulnerabilities of a product. For instance, the smart inhaler connects to the mobile phone of its user and sends a notification about the number of inhalations left. The Bluetooth connection to a mobile phone is considered the devices’ threat. If an attacker connects to the inhaler, he can send unexpected commands and broke the device. Besides, the connection is still needed as it provides better quality of the product. Cybersecurity solution here is denial for inhaler to accept the data, but allow its sending. In addition, here the privacy issue occurs. The data can be sent to everyone who is shown as an owner of the device [Fig. 3].

Fig. 3 Example of user-pretending attack







**Fig. 4** Example of IoT device vulnerability exposure

Another example of security concern in IoT can be vision-improving smart glasses. They automate correction of humans' ability to see and can adapt to brighten lights, make configurations relative to the distance to objects, etc. In one word, they can execute the commands. On the other hand, smart glasses also are able to recognize QR codes. Therefore, the malware code can force this accessory to run the malicious instructions and conduct a ransomware attack (Fig. 4).

Besides, problems of the security-designed approach include limited computation and power capabilities of small and lightweight systems such as wireless sensors, many of these sensors lack built-in encryption that means all data is transmitted in open mode, so anyone who "listens" to the network can get access to it.

In general, privacy means safety of users' personal data. Their consideration of how and what for the private information will be used, who will have access to it, simply – what happens to the information. Moreover, in most countries the legal permission of person is needed for data processing. Therefore, privacy issues are divided into the next categories:

- Data eavesdropping and data confidentiality
- Identity threats
- Unauthorized access to the data
- Inappropriate usage of data
- Location privacy

Besides, network layer in IoT concept is also an area of security issues. Network layer is responsible for data movement; it includes content collecting, delivery and discovery, network addressing, and routing. Network types used by medicine IoT are:

- *Wired or Wi-Fi networks*: connection between gateway and user. They are used by stationary devices and suitable for systems that require high speed.
- *Radio communication (3G, 4G, LTE, Bluetooth, RFID)*: connection between nodes with users and devices. It is used by low-powered IoT mobile devices, usually wearable medicine smart things, and suitable for long distances (cellular based).
- *WSN*: low-powered wireless personal area networks or Wi-Fi for IoT interconnection.

All of the privacy threats may result in significant physical, financial, and emotional harm to the patient; therefore, the privacy-enhancing techniques must not

focus on only one class of threats but also improve overall protection of information in the smart IoT system and system environment in the healthcare industry.

**Data Eavesdropping and Confidentiality** Data eavesdropping also known as a sniffing is a type of passive attack that is hard to determine. By eavesdropping the network where IoT devices communicate and send data, the attacker doesn't need to know any credentials or have physical access to the device. Only unsecure network environment is needed. Data eavesdropping is realized by using sniffers – software for any operation system. Usually, protection against sniffing is avoidance of wireless networks, usage of strong passwords at network access points, and traffic encryption. Specific of IoT devices does not allow the inventors to implement those preventions as it affects the performance. However, researches for privacy-enhancing frameworks [14] or secure communication protocols [8] make us believe that there is a way to protect IoT devices against traffic eavesdropping.

Confidentiality is a property of information to stay in a secret from those who do not have an access permission to it. According to [15] data confidentiality can be improved by using public key encryption (PKI). PKI creates an effective approach to data encryption as it can provide high level of confidence for exchanging information in an insecure environment.

**Identity Threats** Healthcare is a huge environment of privacy threats by itself. The researches of Stephany Domes [16] show that identity breach in healthcare is the largest (67% in the USA in 2015) and the most expensive in the hackers' world. Identity thief can be explained in comparison with credit card thief. When your credit card information was stolen, the attackers got the data about banking account number, amount of money you have, and your pin code, and that is all. Therefore, the exit to the situation is just blocking the card, closing one account, and opening another in a few days. Unlike credit fraud, identity thief in healthcare industry provides to attackers' data about your name, address, employment, insurance, etc.

That information cannot be replaced. It means your identity can be used anytime, so it costs more in the dark net. Nevertheless, there is a positive side: more protection appliances, harder access to personal identity, and law responsibility.

The theft of medical identity, according to the Federal Trade Commission (FTC) [17], happens when someone uses the name and insurance information of another person. They can get medical treatment, prescription drugs, or surgery on behalf of a victim. On the other hand, it can occur when dishonest workers of medical settings submit false bills to insurance companies. Therefore, medical identity theft is a problem for patients and providers of healthcare.

Identity protection is central in privacy security. Mechanisms for information disclosure prevention by Slamaning and Stingle [18] are:

1. Unlinkability – implies an impossibility of attacker to gain any data of links between clients and documents in the system of  $n$  users where the relations of documents  $D$  and users  $U$  exist with probability  $= \frac{1}{n}$ .

2. Anonymity – it is an unidentifiable measure within a set of subjects  $X$ . The rank of anonymity is a scope of the anonymity set  $|X|$ . For instance, anonymity is defined when the anonymous consumer in a set  $U' \subseteq U$  can access document  $D$ .
3. Identity management – a user's identity can be managed by dividing the identity of a person into sub-identities  $I = \{I_{pub}, I_1, \dots, I_k\}$ . Each sub-identity is an alias chosen by the user. A customer can link any sub-identity for any subset of his PHR/EHR records. It helps him to hide confidential information by a sub-identity. Therefore, the data is saved from disclosure attacks.

Hence, the anonymity and pseudonymity techniques can help to hide the real identity of the patients. Further discussion of privacy-enhancing technologies will be given further in the chapter.

**Unauthorized Access to Data** Unauthorized access is an occurrence when someone gets access to a service (website, program, server, or other systems) with someone else's account credentials. For example, if a curious person kept guessing a password and username for an account he didn't own until he gained access, it is unauthorized access to the resource [19].

In case of IoT, the unauthorized access is the first and only step to take control of device. Weak passwords or standard initial passphrases are serious problems in the IoT. The research of Ken Munro [12] has shown that unauthorized access can be gained by looking through the manuals. You do not even need any hacker tools, only connection to the device that is not hard as every smart thing needs to operate through insecure network such as Wi-Fi, Bluetooth, or SSL7 mobile network. Another problem is password-less access. It can appear like a good solution to weak passwords; however, it just simplifies the access to the device. For instance, everyone who uses the same network can connect to the smart system.

The healthcare IoT such as cancer treatment uses a Bluetooth-enabled technology of weight scale and cuff for blood pressure measurement. A symptom-tracking app that manages indicators then sends updates to patients' doctors on symptoms and responses to treatment weekly. However, what can happen if instead of physicians all responses will be sent to the attacker who gained unauthorized access?

Other issue may occur when small security object sends requests to the management system in case of software updates. Such vulnerability was found in the remote control [20]. Attacker turned the device into eavesdropping tool by sending malware to the system while it requested software updates from the broker. The vulnerability persists for almost 4 months that again reminds us about patching problem of IoT devices.

**Inappropriate Usage of Data** Once the attacker gained access to the device or application, he can start using data for his own purposes. It can be money, person manipulation, further movement and usage of the information in other aspects (to involve other people, etc.), or directed harm to the person. Other ways of inappropriate usage of data are intentional or unintentional sharing, interpreting, using information for manipulation, etc. by parts that has rights to access the data.

People often don't ponder about how their personal data can be used. Neither patients nor hospital workers are aware of caution that must be applied when using sensitive information. Sharing patients' data between doctors and nurses is common nowadays. It helps to provide better service. However, the best practices to avoid inappropriate usage of data are accurate legislation regulation and staff education.

## 4 Responsible Parties

When the secrecy of private information was damaged and unauthorized people got access to it, this event is called data leak. Thousands of data leakage are happening every day, some of them are less harmful other more. The forensic process is usually held when most sensitive data was "lost." Its task is to find reasons why data leak has happened, what data was declassified, and who is responsible to that. In this chapter we will quickly look through the first two questions and focus more on the last one as it involves responsibility at the legislative level.

- Why do data breaches happen?

Most of all, the information is declassified unintentionally by humans unaware of unstable confidentiality of the data. Like hospitals, many other organizations are pushed to have an information security policy or confidential policy. However, employers often don't know what it is about and how it must impact their work. Another reason of data leakage is intentional spreading of information when the person understands the importance of privacy and still is due to share it.

- What data became nonconfidential?

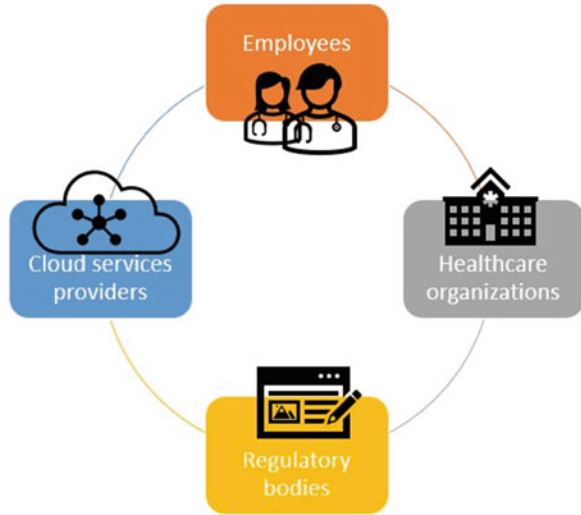
This part may seem the easiest of three, but it is the most important one. Knowledge of what exactly is spreading among people is the key for possible solution. Log notification on the security system or post on the social media, everything that can help to identify the amount of leaked data, should be used to define the next steps for reducing bad consequences.

- Who is responsible to privacy breach?

One of the latest huge data breaches in healthcare happened on March 21st; the Oregon Department of Human Services [21] reported that employees who weren't trained in cybersecurity questions enough had fallen for a phishing attack. Highly sensitive personal data of about 1.6 million people were compromised. This information includes emails, home addresses, names, and much more.

Another big breach has happened recently [22]. Along with a data breach in April 2020, ransomware attack was carried through at one of Fortune's 500 companies, Magellan Health. The healthcare giant admitted that about 365,000 patients were affected by the sophisticated cyberattack. The investigation shows that the attack was a fully planned process with the first step of installing malware to steal employee login credentials. Then the leverage movement stage began to

**Fig. 5** Privacy responsible parties



gain access to the systems of Magellan. Before deploying a ransomware attack, a phishing email impersonated as their clients were sent. Hackers were able to steal the login and password of employees, their ID numbers, personal information, and sensitive patient data such as W-2 information, social security numbers, or taxpayer ID numbers.

A large amount of private data are stolen every day. Information disclosure always includes people; however, we can only imagine the poor security of IoT devices with default credential settings or passwordless access. It means that the stage that goes after people's mistake and must protect the confidentiality isn't well-configured or is absent at all.

According to SciForce [23] taking into account the complexity of the problem and the number of people involved, responsibility level should include members from staff individuals to governments (Fig. 5).

The liability of the parties may be described as follows:

- *Employees*: Employees' ignorance and incaution in cybersecurity matters are first the possibility of hospital IT infrastructure infection. Any other security level doesn't matter if an employee voluntarily sets up malware on his computer or mobile device. Phishing URLs can come from anywhere nowadays, and education of the staff is critical to every organization. Education also must include learning of secure way of using medical devices. For example, workers should consider that medical devices, even those that have a browser with Internet access, cannot be used to surf websites or stream music.
- *Healthcare organizations*: are advised to focus on the security that has been already implemented into medical devices. They also should ensure that the software of connected appliances is updated. Any patch of a critical medical device must assure that it won't cause random problems that may harm a patient.

So, it is vital to manage the latest software installed and be careful about its compatibility.

- *Providers of cloud services*: whereas healthcare organizations are responsible for the secure storage of sensitive data in an encrypted way, they are not able to control the information security over the access points that are used to transmit the data. A significant threat is created with an increasing number of appliances are connected to the network. It should be conducted by communication and data storage providers.
- *Regulatory bodies*: the primary goal for regulatory bodies is the security of personal health information, stored and delivered via connected appliances. To fulfill this need, they need to provide acceptable and consistent legislation.

When some incident happens, it is useful to have a step-by-step plan of what should be done and how to handle it. Therefore, it is worth considering IoT security baselines. The IoT security standards can be part of industrial or governmental regulations. Diving deeper into legislation, next works in security standardizations can clarify the organization process of building the IoT security concept:

- The National Institute of Standards and Technology’s (NIST’s) set of basic [IoT security](#) practices for manufacturers [24]
- The European Union Agency for Cybersecurity’s (ENISA’s) baseline recommendations for IoT [device security](#) [25]
- [Groupe Spéciale Mobile Association’s \(GSMA\) “GSMA IoT Security Guidelines and Assessment”](#) [26]
- The IoT Security Foundation’s “Best Practice Guidelines” [27]

NIST’s publication of IoT security practices is made to help manufacturers to improve the level of security of the Internet of Things. The measurement of how securable device is means its cybersecurity capabilities – features or functions provided by objects’ technical means (hardware and software) – that users need to protect within their systems and environments. It mainly focuses on advices to providers on how they can help customers to manage and reduce cybersecurity risks, what they need to consider during the designing process to help balancing security, and customers’ needs.

Basic IoT security practices consist of four activities with primarily pre-market impact and two activities with primarily post-market impact:

1. Identify expected customers and users, and define expected use cases.

Identifying of users and their expected use cases is essential for determining which cybersecurity capabilities the device should implement and how it should be done.

2. Analyze customer-client cybersecurity needs and objectives.

Risks customer faces determine their security needs and goals. Obviously, providers cannot completely anticipate all risks of their customers. Nevertheless,

providers can make their devices at least minimally secure to those who are expected to use their product consistently and in awaiting use cases.

### 3. Determine how client needs and goals can be satisfied.

Producers can help customers to decrease the cybersecurity risks their organization has. To do that producers have the ability to determine how to satisfy client's needs and goals by providing their IoT devices with particular cybersecurity capabilities. NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline [28], is a publication that goes with a starting point of a device cybersecurity capabilities set that may be needed for customers to achieve their goals and fulfill needs.

### 4. Plan for adequate support of customer needs and goals.

Desired device cybersecurity capabilities can be supported by manufacturers. They need to provision their IoT devices with securable hardware and software resources. Manufacturers should note business resources that are necessary for the development and continued support of the IoT device in ways that support customer needs and goals (e.g., secure coding practices, vulnerability response, and flaw remediation).

### 5. Define approaches for communicating to customers.

Clear communication about cybersecurity risks between manufacturers and customers will be beneficial to both sides. It is important to build a conversation involving security concerns of IoT devices that are currently selling or have been already sold. This communication could be pointed at the customer or other parties acting on the customers' behalf, such as an Internet service provider or a managed security services provider.

### 6. Prepare a plan to communicate and what to tell customers.

When a manufacturer communicates to customers about a particular IoT product, there are many aspects for what information and how that information will be shared. For example, those topics are:

- Cybersecurity risk-related assumptions that the manufacturer made when designing and developing the device
- Software updates, such as if updates will be available, when, how, and by whom they will be distributed
- Support and lifespan expectations, such as expected term of support, what process will guide end of life, will any functions of the device remain after its end of life, etc.

ENISA's baseline recommendation for IoT [device security](#) is a comprehensive work that describes security measurements of IoT in three scopes:

- Policies: security by design, privacy by design, asset management, and risk and threat identification and assessment

- Organizational, people, and process measures: end-of-life support, proven solutions, management of security vulnerabilities and/or incidents, human resources security training and awareness, and third-party relationships
- Technical measures: hardware security, trust and integrity management, strong default security and privacy, data protection and compliance, system safety and reliability, secure software updates, authorization, authentication, cryptography, secure trusted communications, secure interfaces and network services, etc.

Security policies need to be extensive enough to secure IoT used in organizations. Such policies as security by design and privacy by design focus on privacy and security integration on the designing stage rather than adding those properties at the production phase. Organizational, people, and process measures focus on human side of IoT usage. Technical measures are most applicable during development stages. Manufacturers should predict how fast they will sell products and the scalability needed for the chosen security measures.

Provided standards or baselines are only recommendations to manufacturers on how they should handle security while designing, developing, and maintaining their IoT systems. All documents examine cybersecurity as a set of technologies, processes, inventors, and customers. So, while speaking of responsible parties for preventing data leakages or managing security breaches, we need to remember about every human part of IoT environment.

## 5 Privacy-Enhancing Technologies

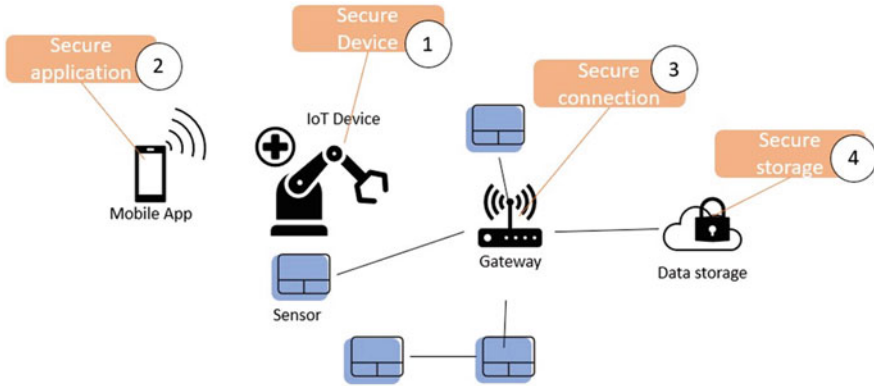
Cybersecurity specialists are working every day on new technologies to protect us in cyberspace. Confidentiality is one of three main properties of information; the others are availability and integrity. Privacy issues are mainly directed to confidentiality – it is a property of information to be accessible only by users who has permission to that. According to IBM [29], cybersecurity is a set of comprehensive approaches:

- Technical controls (T): network infrastructure, endpoints, servers, identity management, vulnerability management, monitoring, and logging
- Administrative controls (A): policies, procedures, standards, user education, incident response, disaster recovery, compliance, and physical security
- Asset management (AM): classification, implementation steps, asset control, and documentation

Hence, we can combine different approaches to classify IoT privacy protection. According to [14] privacy protection and prevention approaches are:

- Minimization of data: the collection is limited to only necessary information (A).
- Data anonymization: applying techniques like encryption and modification or personal data removal in such a way that decreases the possibility of persons' identification (T).





**Fig. 6** Placing of privacy-enhancing technologies

- Data security: data protection from corruption and unauthorized access (A, T, AM).
- Data control: defined policies for data monitoring and controlling (AM).
- Identity management: protection of user identity by policies and technologies that grant access to resources only to the legitim users (A, T).
- Secure communication: communication protocol that provides confidentiality, integrity protection, and source authentication (T).
- User awareness: contests of user awareness about what data are processed and how it is used (A).

According to [14] the privacy-enhancing technologies can be categorized by where they are placed [Fig. 6]:

1. Implemented in devices: means that security technologies are built-in by the manufacturer.
2. Used as applications: e.g., implemented by user side.
3. Applied in networks: network devices are responsible for privacy in the interconnected system.
4. Applied in data storage, cloud, and back-end servers: privacy protection for data in rest.

IoT privacy-enhancing technologies by [1] are:

- Encryption.
- Secure boot.
- Security measures that should be an integral part of the design of the IoT device. It includes managing risk assessment before the device is released for use in the market; authentication measures should be built into the device.
- Principle of least privileged implementation. Proper following of authentication, limited device access, firmware verification, and monitoring of device-to-device communication.

- Strategy of defense. It might comprise several security layers that are in place to protect against specific risks.
- Proper access control assurance in place that limits unauthorized access to data, IoT devices, and networks.
- Audit and testing of the IoT device security before it's put in production and continuous monitoring of device security throughout its life cycle.
- Establishing a security culture, with regular employees' education to recognize vulnerabilities.

Other technologies are discussed deeper.

**Encryption and Communication Protocols** Among times, encryption is the way of hiding data from others. It is base security approach to ensure privacy. Traditionally information exists in movement – while it is transmitted through the network, data in rest and while it is saved in database, hard drive, etc., data in use – the state of information that is currently in the process. We can apply encryption while data is passively stored or transmitted. The IoT architecture makes the collecting devices to transfer data once they gained it; however, it still must be saved during the synchronization interval. Solution that is more practical is an encryption of end systems as data storages and can be achieved by using an endpoint encryption services. Interesting stage here is encryption followed by authorization at transport layer.

Traditional encryption technique doesn't suit computational requirements of IoT. It has limited resources to provide accurate authorized connections, to store certificates and trusted parties' public keys, or generate signatures as traditional computers do. Several transport protocols are widespread among different models of IoT communication platforms. They must provide data security in movement.

Message Queuing Telemetry Transport (MQTT) is lightweight publication/subscription type (pub/sub) messaging protocol that works over TCP/IP. It is the most popular protocol among IoT devices. MQTT is based on subscriber, publisher, and broker model. Within the model, the publisher's task is to collect the data and send information to subscribers via the mediation layer which is the broker. On the other hand, a broker has the role of ensuring security by cross-checking the authorization of publishers and subscribers. Quality of Service (QoS) helps to achieve that by providing three possible levels:

- QoS0 (at most once): The least reliable mode but also the fastest. The data is sent but confirmation is not received.
- QoS1 (at least once): Ensures that the message is delivered at least once, but may cause duplicates.
- QoS2 (exactly once): The most reliable mode and at the same time the most bandwidth-consuming. Duplicates are controlled to ensure that the message is delivered only once.

Those approaches of transport protocol offer minimum bandwidth usage, operation over wireless networks, low energy consumption, and good reliability if

necessary. Nevertheless, the origin implementation of MQTT doesn't provide encryption as TCP doesn't do it. Only payload data can be encrypted. Moreover, the TLS usage is not feasible for constrained devices in most IoT scenarios [30]. TLS is both computationally heavy and may require high memory usage.

However, [8] offered a secure version of it. Elliptic Curve Integrated Encryption Scheme, a modified elliptic curve variant of the Schnorr digital signature scheme, the Rabin encryption cryptosystem, and Advanced Encryption Scheme in an authenticated mode is a base of the secure MQTT. Secure MQTT focuses on security levels opposed to Quality of Service. Setup and join phases are prior to the communication phases which differentiates according to security level provided.

Data distribution service (DDS) designed by Object Management Group [31] is another popular IoT protocol that is spread in industrial IoT including healthcare service. DDS can be used for the management of data exchange either between a set of lightweight devices or the interconnection of large, high-performance sensor networks. It also supports cloud integration (e.g., send and receive data from the cloud). It combines together the components of a system; therefore, it provides low-latency data connectivity, maximal reliability, and scalable architecture that are needed by the business and critical IoT applications. DDS consists of four layers of domains and each of them is responsible for its own purpose. For example, machine domain includes sensors, machine elements, and devices, which collect and transmit data. Mechanisms included in DDS provide authentication, access control, integrity, and confidentiality to the information distribution. DDS security uses a decentralized peer-to-peer architecture. Thanks to that, it affords security without sacrificing real-time performance. That means any security techniques such as encryption or authentication can be accessed by usage of special plug-ins. Despite numerous plug-ins the DDS security is complex to administrators and needs high-skilled staff for configuration.

Other protocols exist and are used in IoT environment such as Constrained Application Protocol (CoAP), ZigBee, and Lightweight M2M (LwM2M), but they aren't so popular in healthcare sector.

**Secure Boot** Secure boot implies confidence that device wasn't touched or somehow modified during turn-off stage. It also means that official last update of IoT operating system was installed. Zero-trust model principle says: "Find the simplest part of the device which you can trust and start build secure system around it." But, we usually must trust new devices we get from the shop. So, perimeter protection, system updates, and secure configuration are a minimum to provide secure boot technology.

**Access Control** Another approach of healthcare IoT protection is using suitable access control model. Access by pre-defined roles for each system in the IT environment is called role-based access [32]. Capability-based means privileged access to the objects in the network [33]. Attribute-based access control works by checking the attributes for each system in the network [34]. Alshehri and Sandhu introduced the architecture for cloud-based IoT [35]. All models reduce the illegal behaviors in the network despite specific problem solution they provide. Case

study [36] introduces the new security model that adds the edge layer in the cloud IoT infrastructure, which gives real-time decision and controls the data sources. However, the edge computing services except its benefits add more security and privacy challenges. Therefore, additional privacy policies usage is a must. They will regulate message-passing protocol, point-to-point encryption at each level, and specific X509 certificates to make sure there is less data spying.

**Risk Assessment and Security Measurements** Risk assessment or qualifying of security level is important in the IoT, because it can improve security standard level not only in healthcare sector but in other areas as well. The level of security and privacy in the Internet of Things solutions is not completely measured for customers who have already implemented them in their infrastructure. Therefore, new users can't compare and choose systems based on their privacy and security requirements. On the other side, usage of assessment criteria without demanding attention to some important aspects of the IoT security offerings, such as hardware security, mobile applications, and web also, limits qualified estimation of risks for privacy in IoT. Therefore, the goal question metric by [37] is right solution of security and privacy assessment. It describes goals as components of IoT infrastructure, so the edge goal can be medical sensors, wearable IoT, or stationary devices. The gateway is a network-providing device, and the back end is usually described as cloud-based platform with mobile application or web interface access. Each goal has either its own security properties or sub-features as well. After that the questions based on OWASP, CSA, GSMA, and other cybersecurity organizations were provided. The metrics gives a result of security and privacy assessment. Assessment process is shown at Fig. 7. Further computational details are accessible at [37–39].

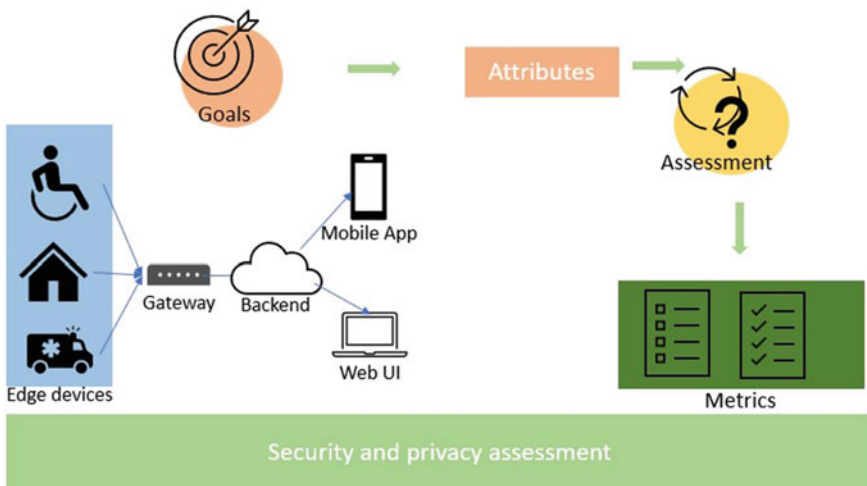


Fig. 7 Security and privacy assessment process

Therefore, a range of security approaches exists in the IoT area. However, it has research potential and ways for improvement [40–44].

## 6 Conclusion

In this chapter the following were discussed: healthcare IoT services and applications, the role of IoT in healthcare; privacy issues that occur when using IoT in healthcare and main attack vectors for gaining information, eavesdropping, unauthorized access, identity threats, inappropriate usage of data, and location privacy; responsible parts of data confidentiality protection, employees, healthcare organizations, providers of cloud services, and regulatory bodies; privacy-enhancing technologies which should not affect the efficiency but protect information processed by IoT devices in healthcare; and comprehensive cybersecurity approaches and privacy-enhancing technologies.

## References


1. A. Chacko, T. Hayajneh, Security and Privacy Issues with IoT in Healthcare, in *EAI Endorsed Transactions on Pervasive Health and Technology*, July 2018
2. Cybersecurity policy for the Internet of Things. <https://www.microsoft.com/en-us/cybersecurity/contenthub/cybersecurity-policy-for-IoT>, 2019
3. S.M.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K. Kwak, The internet of things for health care: A comprehensive survey. *IEEE Access* **3**, 678–708 (2015). <https://doi.org/10.1109/ACCESS.2015.2437951>
4. J. Conway, The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise Schneider Electric Whitepaper (2015), p. 2
5. L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, M. Vento, Trends in IoT based solutions for health care: Moving AI to the edge <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7217772/#:~:text=IoT%20solutions%20for%20healthcare%20are,recognize%20activities%20and%20making%20decisions>
6. Dr. Dennis Ong, IoT and Machine Learning - Changing the Future, TEDx Talks, 2018., [https://www.youtube.com/watch?v=mIE03Fj2T9s&ab\\_channel=TEDxTalks](https://www.youtube.com/watch?v=mIE03Fj2T9s&ab_channel=TEDxTalks)
7. Flatworld Solutions, Top 10 applications of machine learning in healthcare. <https://www.flatworldsolutions.com/healthcare/articles/top-10-applications-of-machine-learning-in-healthcare.php>
8. L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, Radek Fujdiak A Secure Publish/Subscribe Protocol for Internet of Things, *ARES '19: Proceedings of the 14th International Conference on Availability*, 2019
9. S. Domes Protecting Medical Devices from Cyberharm, TEDx Talks, 2016., [https://www.youtube.com/watch?v=EyqwUFJKZo0&ab\\_channel=TEDxTalks](https://www.youtube.com/watch?v=EyqwUFJKZo0&ab_channel=TEDxTalks)
10. Secure healthcare records, ensure patient safety and hospital operations, Check Point Software Technologies Ltd, 2020., <https://www.checkpoint.com/downloads/products/cp-IoT-security-healthcare-solution-brief.pdf>
11. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: Perspectives and challenges. *Wirel. Netw* **20**(8), 2481–2501 (2014)

12. K. Munro, Internet of Things Security, TEDx Talks, 2018., <https://www.youtube.com/watch?v=pGtnC1jKpMg>
13. P. Dutta, 5 biggest data breaches of 2020, Security Boulevard, 2020., <https://securityboulevard.com/2020/08/5-biggest-data-breaches-of-2020-so-far/>
14. L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, S. Ricci A Privacy-Enhancing Framework for Internet of Things Services, Network and System Security, 13th International Conference, 2019,
15. Wassnaa AL-mawee, *Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey* (Western Michigan University, 2012)
16. S. Domes, Protecting medical devices from Cyberharm, TEDx Talks, 2016., [https://www.youtube.com/watch?v=EyqwUFJKZo0&ab\\_channel=TEDxTalks](https://www.youtube.com/watch?v=EyqwUFJKZo0&ab_channel=TEDxTalks)
17. Federal trade commission <https://www.ftc.gov/>
18. D. Slamanig, C. Stingle, Privacy Aspects of eHealth, IEEE 3rd Int. Conf. on Availability, Reliability and Security, Barcelona, 2008
19. Computer hope, 2020., <https://www.computerhope.com/jargon/u/unauacce.htm#:~:text=Unauthorized%20access%20is%20when%20someone,it%20is%20considered%20unauthorized%20access>
20. J.J. Lehmann, *WareZTheRemote: Turning remotes into listening devices* (Guardicore, 2020)
21. Associated Press, *Oregon department of human services confirms data breach* (The Register Guard, 2019) <https://selfkey.org/data-breaches-in-2019/>
22. J. Davis, *Magellan Health Data Breach Victim Tally Reaches 365K Patients* (Health IoT Security, 2020) <https://healthitsecurity.com/>
23. Sciforce, *Ensuring privacy and security in the healthcare IoT* (Sciforce article, 2019) <https://medium.com/sciforce/>
24. M. Fagan, K.N. Megas, K. Scarfone, M. Smith, Foundational cybersecurity activities. National Institute of Standards and Technology Interagency or Internal Report **8259** (2020). <https://doi.org/10.6028/NIST.IR.8259>
25. Baseline Security Recommendations for IoT, 2017.: <https://www.enisa.europa.eu>
26. GSMA IoT Security Guidelines, 2016.: <https://www.gsma.com/IoT>
27. Daudid, Establishing principles for Internet of things security, IoT Security Foundation: <https://www.IoTsecurityfoundation.org>
28. M. Fagan, K. N. Megas, K. Scarfone, M. Smith, IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A, 2020. <https://doi.org/10.6028/NIST.IR.8259A>
29. IBM: <https://www.ibm.com>
30. T. Heer, O. Garcia-Morchon, R. Hummen, S. Loong, Keoh, S.S. Kumar, K. Wehrle, Security challenges in the IP-based Internet of Things. *Wirel. Pers. Commun.* **61**(3), 527–542 (2011)
31. DDS by OMG: <https://www.dds-foundation.org/what-is-dds-3/>
32. R.S. Sandhu, Role-based access control, in *Advances in computers*, (Elsevier, 1998)
33. J.L. Hernández-Ramos, A.J. Jara, L. Marin, A.F. Skarmeta, Distributed capability-based access control for the internet of things. *J. Internet Serv. Inf. Secur. JISIS* **3** (2013)
34. C. T. Hu, et al., Guide to Attribute Based Access Control (ABAC) definition and considerations [includes updates as of 02-25-2019], 2019
35. A. Alshehri, R. Sandhu, Access control models for cloud-enabled internet of things: A proposed architecture and research agenda, in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, (2016)
36. M.A. Tawalbeh, L. Tawalbeh, M. Quwaider, *Authorization Model for IoT Healthcare Systems: Case Study* (Conference Paper, 2020)
37. F. Alsubaei, A. Abuhussein, S. Shiva, Quantifying security and privacy in internet of things solutions, 2018 International Conference on Cyber Physical Systems and IoT (CPSIoT 2018), Stockholm
38. L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, S. Ricci, A privacy-enhancing framework for internet of things services, in *International Conference on Network and System Security*, (Springer, Cham, 2019 Dec 15), pp. 77–97

39. A.D. Dwivedi, L. Malina, P. Dzurenda, G. Srivastava, Optimized blockchain model for internet of things based healthcare applications, in *2019 42nd international conference on telecommunications and signal processing (TSP)*, (IEEE, 2019 Jul 1), pp. 135–139
40. Z. Wang, D. Wu, R. Gravina, G. Fortino, Y. Jiang, K. Tang, Kernel fusion based extreme learning machine for cross-location activity recognition. *Inform Fusion*. **37**, 1–9 (2017 Sep 1)
41. G. Fortino, A. Guerrieri, F. Bellifemine, R. Giannantonio, Platform-independent development of collaborative wireless body sensor network applications: SPINE2, in *2009 IEEE International Conference on Systems, Man and Cybernetics*, (IEEE, 2009 Oct 11), pp. 3144–3150
42. C. Savaglio, P. Pace, G. Aloï, A. Liotta, G. Fortino, Lightweight reinforcement learning for energy efficient communications in wireless sensor networks. *IEEE Access*. **7**, 29355–29364 (2019 Mar 4)
43. C. Ma, W. Li, R. Gravina, G. Fortino, Posture detection based on smart cushion for wheelchair users. *Sensors* **17**(4), 719 (2017 Apr)
44. S. Iyengar, F.T. Bonda, R. Gravina, A. Guerrieri, G. Fortino, A. Sangiovanni-Vincentelli, A framework for creating healthcare monitoring applications using wireless body sensor networks, in *Proceedings of the ICST 3rd international conference on Body area networks*, (2008 Mar 13), pp. 1–2

# Intelligent IoT for Automotive Industry 4.0: Challenges, Opportunities, and Future Trends



Raj Krishan Ghosh, Anindya Banerjee, Prasenjit Aich, Deborsi Basu,  
and Uttam Ghosh 

## 1 Introduction

In recent years, the IoT revolution (Internet of Things) has changed the way industries are working [1]. A wave of smart technologies like artificial intelligence, machine learning, deep learning, cloud and edge computing, federated learning, and automation hit the conventional IoT and govern the idea of Intelligent IoT, which is the key technology enabler in Industry 4.0. IoT, which means the interconnections among devices with embedded sensors, actuators, and software, now becomes over five decades old. IoT also changes its applications, appearance, and impacts with upgraded concepts and methodologies in the real world. The IoT Analytics report states that by the end of 2018, over 7 billion devices have been connected via IoT modules [2]. Similarly, Cisco IBSG predicts 50 billion devices connected via the IoT by 2020 [3]. It comes out to be an obvious fact that big industries are inundated with data that are generated by these interconnected devices. They are looking for smart

---

R. K. Ghosh

Center of Excellence in Artificial Intelligence, Indian Institute of Technology Kharagpur,  
Kharagpur, West Bengal, India

A. Banerjee

Department of Electronics and Communication Engineering, Kalyani Government Engineering  
College, Kalyani, West Bengal, India

P. Aich

Mphasis Limited, Mahadevapura, Bangalore, India

D. Basu (✉)

G. S. Sanyal School of Telecommunication, Indian Institute of Technology, Kharagpur, India

U. Ghosh

Dept. of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN,  
USA

e-mail: [uttam.ghosh@vanderbilt.edu](mailto:uttam.ghosh@vanderbilt.edu)



AI-ML-based solutions capable of managing, storing, processing, transmitting, receiving, and updating a large amount of data efficiently. The critical point is to extract meaningful information from the data and only keep the genuine information by discarding the redundant data. The Intelligent IoT system aims to enable the companies to deliver user-friendly products as per the customers' needs. The concept of Intelligent IoT also triggers concepts like the Internet of People (IoP), Internet of Vehicle (IoV), Internet of Softwarized Things (IoST) [4, 5], Internet of Everything (IoE), etc. IoT's relationship with all the latest AI-based technologies is changing many industries to procure their respective objectives. In the twenty-first century, enterprises are always aiming to apply digital transformations inside their conventional business model. The reformation of industry outlook due to IIoT is responsible for fetching the customers' immense attention by customizing user experience, optimizing productivity, and obtaining analysis with insights and predictions. The dynamic flexibility plays a vital role in Industry 4.0, using which a smooth up-gradation and addition of advanced technologies are done. IIoT devices give systems an actual interface to the real world. The global application range in all domains of science and technology of IIoT makes it industry-ready. The digital convergence of manufacturing/production and associated sectors, as well as value generation processes, corresponds to Industry 4.0. Industry 4.0 is a new step in organization and control of the global supply chain [6]. It is used interchangeably with the fourth industrial revolution [6]. The digital impact of the industrial revolution has been demonstrated in this chapter. From the simple IoT models to advanced IIoT models, all the application areas are covered with suitable examples and real research outcomes. This chapter's primary objective is to provide a beginner fundamental idea of the evolution of IIoT to conventional IoT technology. The chapter organization has been explained in detail below.

**Chapter Organization** The rest of the chapter is organized as follows: Section 2 introduces Intelligent IoT. Section 3 elaborates the applications of IoT for better social life, to improve healthcare and personalized use of IoT, while Sects. 4 and 5 briefly discuss the applications of IoT using image processing and computer vision and applications of IoT in automotive industry, respectively. Sections 6 and 7 elaborate the role of AI and ML in IoT, respectively, and briefly discuss the corresponding algorithms' basics. Sections 8 and 9 draft the theory of neural networks, deep learning, transfer learning, and CNN. Section 10 discusses the recent breakthroughs of IoT. In Sect. 11, few IoT-based smartphone applications and their uses have been described. Section 12 briefs the current challenges of implementing IoT in real-time applications and also discusses the future opportunities of the same. Section 13 concludes with a summary of the topics explained in this chapter.

## 2 Concept of Intelligent IoT

Technologies transform our lives and play a vital role in making more and more achievements accessible. A relatively new emerging technology, the Internet of Things (IoT), also known as machine-to-machine (M2M) technology, offers both opportunities and promises. These are defined by the networks where smart machines gather data, transmit information across each other, process the data collaboratively, and take appropriate action by themselves. One addition, in particular, is the usage of artificial intelligence (AI) in IoT, popularly known as Intelligent IoT. This technology relies on machines mimicking human thinking and decision-making to provide better and more personalized services that are more accurate and reliable [6].

AI plays a vital role in IoT uses and utilizations. Major dealers of IoT offer integrated AI abilities such as analytics based on machine learning (ML). The importance of AI in such applications is to extract inferences from a large amount of data. Thus, ML brings the capability to automatically find patterns and notice differences in the figures that smart sensors and smart devices generate. The information generated can vary according to the use, such as temperature, humidity, pressure, sound, air quality, or vibrations. In contrast to traditional intelligence tools for business, which typically look out for thresholds to be crossed, ML approaches can easily make predictions at much faster rates and with greater accuracy.

Intelligent IoT is being developed for a variety of real-world applications, including smart transportation and smart cities, to make human life more reliable. With the growth of the Internet of Things, a massive amount of sensing data is produced by numerous sensor devices. AI plays a major role in the study of big data as a comprehensive analytic method that allows for a flexible and accurate investigation of statistics in real time. The creation and expansion of a useful big data tool for AI research face unique challenges, including central infrastructure, security, confidentiality, resource constraints, and a lack of suitable training data [7].

Sensing, transmission, computations, and networking machinery continue to create an increased amount of data, and the trend is likely to continue in the upcoming years. Future Intelligent IoT could, specifically, be used mainly in tasks including but not limited to medicine, environmental monitoring, healthcare, and city management, requiring data handling, the extraction of information, and making real-time decisions. Cloud computing only by itself cannot maintain such general placements and applications as a result of infrastructure inadequacies such as limited transmission bandwidth, intermittent network connectivity, and limitations relating to massive delays. To address these challenges and ensure timely and appropriate data processing and versatile services, multitier computational resources are needed, which have to be deployed and pooled along the cloud range to the physical entities.

### **3 Comprehensive Applications of Intelligent IoT**

Intelligent IoT is a versatile technology and finds applications in almost all life areas, ranging from improving the lifestyle and quality of healthcare to more reliable and sophisticated automation systems. The practical implications are endless and bound to yield better quality of life as the technology matures and progresses [6]. The broad categories of applications are summarized below.

#### ***3.1 Applications That Save Time and Resources***

Embedded sensors in our homes will recognize human actions and accurately monitor air temperatures and lighting to reduce our energy consumption without sacrificing human comforts. In the case of a farm field, faraway bug traps can detect an outbreak of insects and pests and, as a result, begin spreading the appropriate amount of pesticide. Not only would this reduce the risk of overspreading, but it will also reduce the risk of crop disruption. Intelligent IoT can thus be used for smart houses, smart route planning, intelligent construction, economic agriculture and breeding, supply chain automation, fleet management, and factory automation, among other things. Furthermore, it can be used in a variety of sectors, including nice, commodity, and shipping monitoring, efficient natural resource extraction and transportation, efficient energy and water production and usage, smart metering and billing, and traffic control.

#### ***3.2 Applications for Better Lifestyle***

Sensors added to a vehicle will assist drivers in recognizing the possibility of colliding with one another. Typically, inter-vehicle communications and sensors enable us to identify features that would otherwise be impossible. We will mitigate automobile crash rates by using timely and appropriate alert systems, and therefore the technology promises vehicle protection. Factory protection, natural hazard alert, infrastructure surveillance, homeland security, unmanned defense, emergency management system, and building safety and security are among the other areas covered.

#### ***3.3 Applications That Improve Healthcare***

The Intelligent IoT-enabled sensors will help us track elders' health and offer appropriate assistance, such as alerts of elevated blood pressure warnings, demanding

medical assistance, and skipping a dosage. Assistive living, nutritional screening, environmental protection, food and drug tracking and identification, and chronic illness management are examples of healthcare applications [8].

### ***3.4 Applications for Personalization***

Intelligent IoT can provide various personalized experiences for the user, including but not limited to smart entertainment, self-learning games and applications, as well as intelligent signage and shopping recommendation.

## **4 Intelligent IoT in Image Processing, Pattern Recognition, and Computer Vision**

Internet of Things (IoT), image processing, pattern recognition, and computer vision have been widely used for solving various industrial problems independently. The combination of these techniques is yet not explored subsequently [9]. Some of the applications of IoT in various domains are shown in Fig. 1. A combination of these techniques to solve various real-world problems has been discussed briefly:

- Utilizing computer vision with IoT for home security applications is possible by monitoring people's movement and by facial recognition. A passive infrared sensor (PIR) embedded on Raspberry Pi is used to detect the movements with a digital camera's help. The suspicious images are sent to a smartphone [10].
- To curb the excess energy consumed daily by using home appliances, the application of IoT sensing networks combining with image processing is quite useful. This can be done by identifying human activities through image processing and utilizing energy supply as required by IoT.
- Metro cities with busy roads, frequent loading, and unloading trucks cause road congestion and traffic nuisance. IoT-based surveillance system is highly beneficial to alleviate these kinds of problems. Real-time images of truck loading and unloading and traffic congestions are captured through a computer vision-based surveillance system, and the relevant data is transmitted through IoT-based networks [11]. This is highly effective for efficient traffic management.
- Industrial parameters like pressure level, voltage supply of the equipment, temperature reading of a machine, and management can be monitored using IoT, image processing, and machine learning. The controlled hardware part acts as a central processing unit by using Arduino mega. These techniques are completely safe and effective for both large-scale and small-scale industries [12].

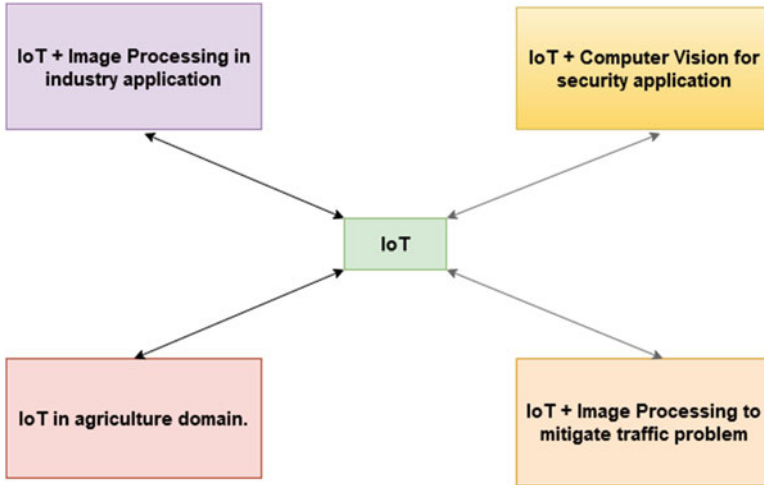


Fig. 1 Applications of IoT in a Different Domain

## 5 Intelligent IoT in Automotive Industry

With the latest research in technologies including wireless distributed sensor, embedded system, smart cognitive radio networks, lightweight material, higher efficiency and ultralow emission internal combustion engines, cloud computing, high-performance battery and fuel cell technology, and intelligent converter, there is a possibility of the production of safer, smarter, zero-emission, and energy-efficient vehicles in the upcoming years. Apart from automobile technologies, other aspects such as users on the road, proper road infrastructures, well-sustained vehicles, attitudes of drivers, and the presence of rules and regulations are also to be taken into account, and they need to work together to preserve our natural and maintain clean environment and sustainably produce mobility [13].

Embedded memories often play a significant role in enabling mobile applications, IoT, high-performance computing, and security [14]. The semiconductor business is tactically concentrating on automotive and industrialized markets. The substantial venture is directed to address these types of markets. The automotive industry, mainly, is in focus for the last numerous years already. With its endless potentials in Intelligent IoT applications, industrial markets are getting an increased amount of attention as construction automation, workshop automation, and grid structure rapidly progress [15].

Automotive software used in modern locomotives and vehicles is getting very complex, and numerous new features and opportunities are offered. Manufacturers' main problem is to ensure that new features, bug fixes, and improvements are quickly applied to vehicles, as current software updates in repair shops are not practical [16].

## 6 Artificial Intelligence in Intelligent IoT

Artificial intelligence (AI) is defined by the simulation of human thinking and intelligence in machines, which are programmed to think and decide like humans and thus mimic their decisions. AI is recognized by the automation of jobs related to humanlike thinking, including decision-making, problem-solving, perception, learning, and reasoning [17]. AI's objective is to justify and perform to result in the best likelihood of accomplishing a specified target. AI is built upon the notion that a human's intellect can also be defined from a direction that machines can simulate to accomplish jobs, from the easiest to those that are immensely complex. As technology progresses, newer standards render the former ones trivial and insignificant. Consequently, AI is uninterruptedly developing as an artificial rational entity to assist an enormous number of massively dissimilar industries [18] (Fig. 2).

Algorithms often have a very significant role in the building of AI. Simpler algorithms are generally sufficient for use in simple applications, while difficult ones develop robust AI. Several of the most commonly used algorithms related to AI include fuzzy logic (FL), adaptive fuzzy logic (AFL), expert systems (ESs), and genetic algorithms (GAs).

Expert systems are essentially an attempt to imitate humans' thought processes through the representation of inference and knowledge mechanisms. Inside a destined domain for knowledge, ESs are adept at making judgments with quality comparable to human experts [19] (Fig. 3).

In FL, the demonstration of knowledge is related more firmly to how humans think. FL has the proficiencies of robust inference of ESs in addition to the natural (linguistic) depiction of knowledge. FL is already realized effectively in applications related to control where either system models do not exist or models are computationally intensive and mathematically complex. AFL is a fuzzy logic-based model that holds the abilities of optimization related to GAs, enhancing the

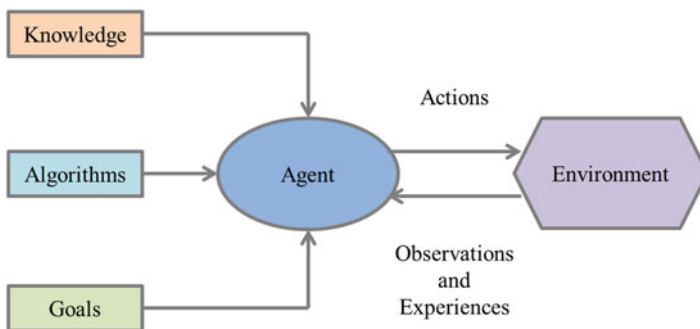


Fig. 2 Basic Block Diagram of an AI System

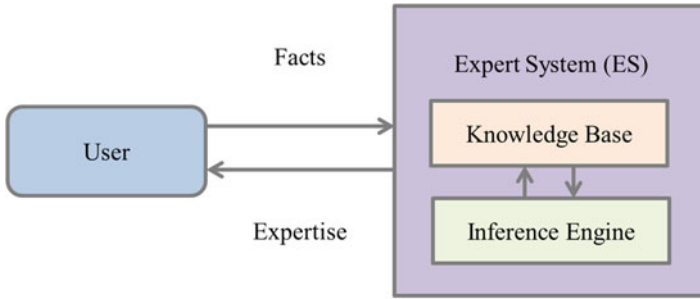


Fig. 3 Block Diagram of an Expert System (ES)

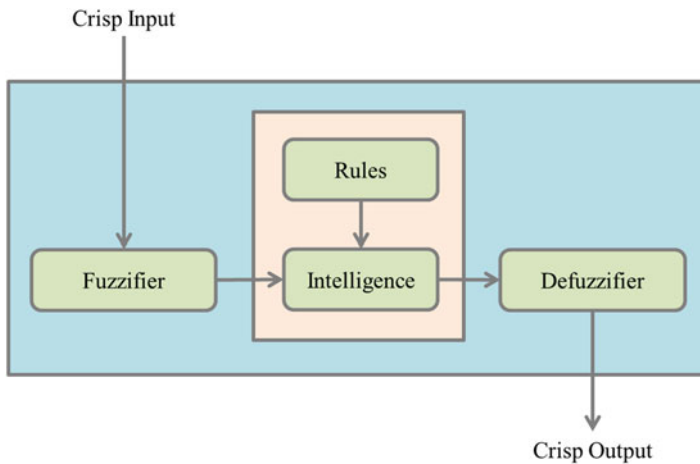


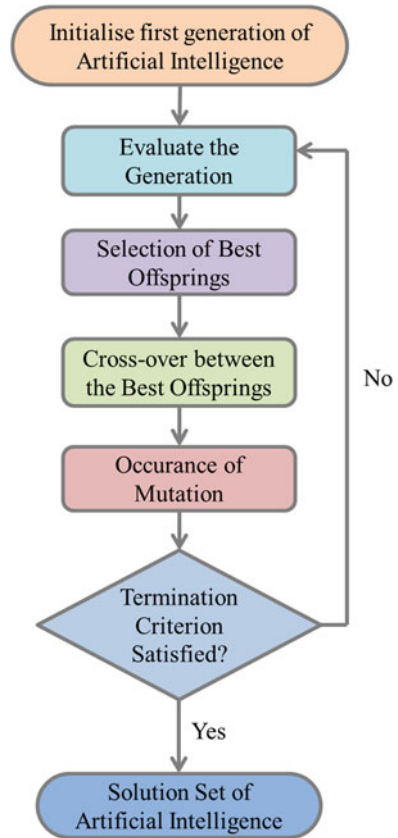
Fig. 4 Block Diagram of a Fuzzy Logic (FL) System

performance of intelligent systems by using some knowledge beforehand [20, 21] (Fig. 4).

GAs use the concept of genetic evolution techniques of real-life organisms to generate optimum results. GAs are occasionally identified as a multidimensional optimization method built upon a genetically random search engine [22] (Fig. 5).

The uses for AI systems are seemingly boundless. The technology can assist healthcare manufacturing to dose drugs, for diagnosis and surgeries; in automotive industry which includes cars and self-driving wheelchairs; financial business in detection and prevention of deception. These machineries must resolve the best sequence of action for whatever decision is taken by them, as every action will influence the result at the end [23]. For instance, self-driving cars should necessarily care for all external inputs and perform to confirm the prevention of any crashes. Thus, AI is continuously modifying and is an ever-growing technology.

**Fig. 5** Flowchart of a Genetic Algorithm (GA)



## 7 Machine Learning in Intelligent IoT

Machine learning (ML) is an essential subset of artificial intelligence (AI). The systems can learn automatically and advance from situations without explicitly being programmed for it. ML emphasizes the evolution of computational programs that access the available data and learn by themselves [24] (Fig. 6).

The ML procedure uses existing data, more popularly known as training sets, to notice, evaluate, and gain familiarity in likelihood by considering for patterns. Sometimes, this is accompanied by the presence of a reward function and a cost function for the artificial investigation in many of the available training sets. The structure iteratively rectifies itself over the whole training set. The objective here is to allow the systems without any human interaction to learn automatically [25]. After analyzing all the training sets, the methods then predict the result or make choices based on the data’s information: the more the available training sets, the better the predicting ability. Algorithms corresponding to ML are most often



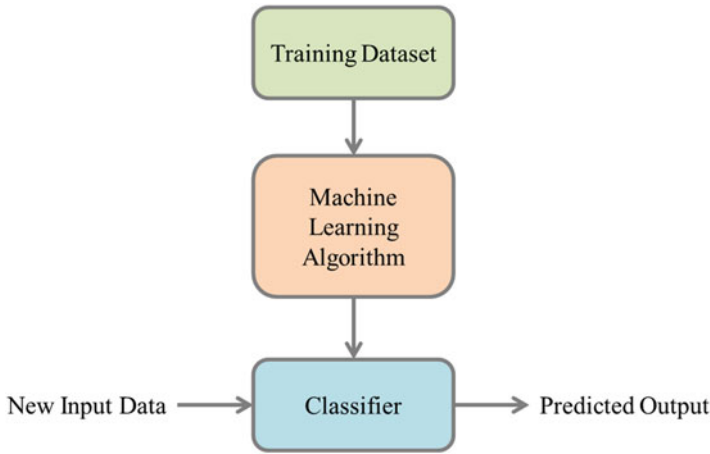


Fig. 6 Basic Block Diagram of Machine Learning

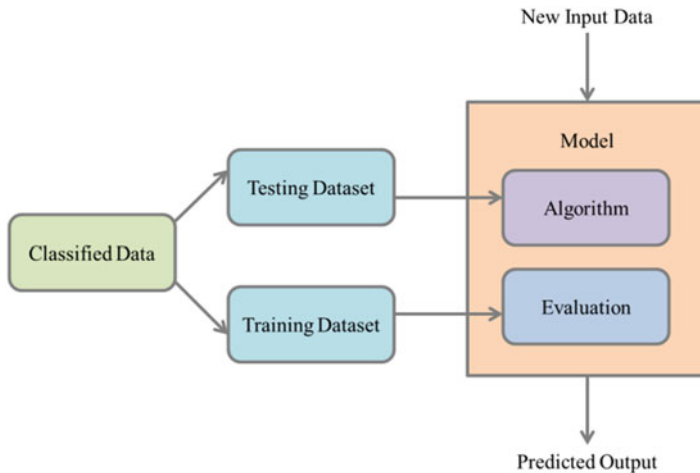
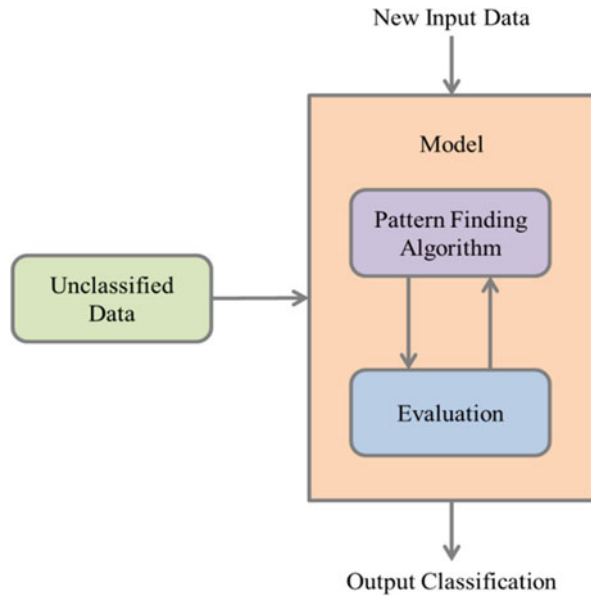


Fig. 7 Block Diagram of Supervised Machine Learning

classified as supervised ML, semi-supervised ML, unsupervised ML, and reinforced ML [26].

Supervised ML algorithms and programs make decisions based on learning and correcting steps used in training sets to new data to predict future events and consequently take proper decisions. The algorithm then associates a specific function to make prognoses for the expected outputs starting with the already known training set analysis. The algorithm can also compare the correct output to detect parametric deviations to adjust the model accordingly to minimize the cost functions [27, 28] (Fig. 7).

**Fig. 8** Block Diagram of Unsupervised Machine Learning

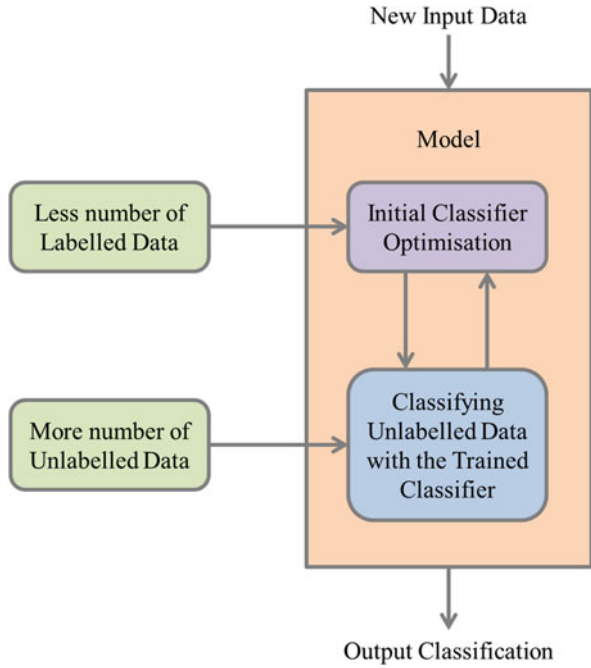


Unsupervised ML algorithms are employed when data utilized for system training is not classified. Mechanisms using this learning procedure also study how to determine a function to describe a structure hidden deep inside the training sets. Unsupervised algorithms do not necessarily focus on inferring specific decisions for the output but rather attempt to search for patterns underlying the data. Therefore, they often discover new criteria and criteria for sorting purposes and classifying the data [29, 30] (Fig. 8).

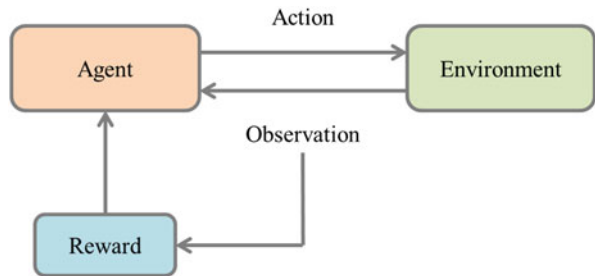
The semi-supervised ML algorithms, in particular, use the features of both the supervised ML and unsupervised ML procedures for training to use both classified and unclassified training datasets for better learning outcomes. Typically, unclassified or unlabeled data turns out to be much larger compared to labeled or classified data. Semi-supervised learning has an added advantage over unsupervised and supervised learning since learning accuracy is much better. These learning algorithms can also be implemented when training set data is incomplete, often the case in real life, and have absent entries for classification [31] (Fig. 9).

Reinforcement ML algorithms use reinforcement signals, often treated just like rewards or otherwise as punishments, corresponding to decisions that are made by the program. In principle, an analogy can be found by taking an example of making a pet learn good and bad behavior by presenting rewards for right actions and similarly punishments for wrong actions performed. The presence of reward feedback ensures the proper identification of mistakes and helps the program choose the best paths for the iterative learning approach. Therefore, the system continuously applies iterative changes for the parameters to maximize the performance-based upon rewards or punishments it receives [32, 33] (Fig. 10).

**Fig. 9** Block Diagram of Semi-Supervised Machine Learning



**Fig. 10** Simplified Block Diagram of Reinforced Machine Learning

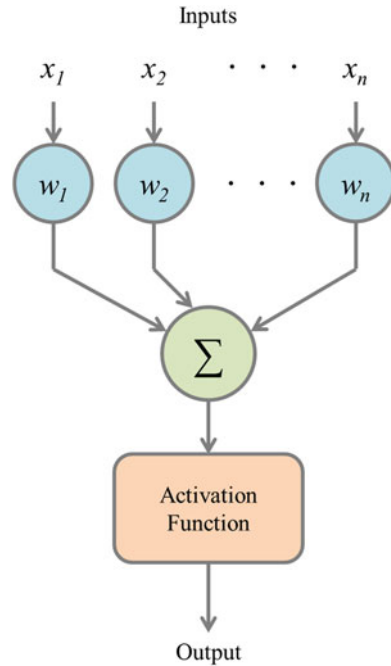


ML, while giving quicker and more accurate results in most cases, also needs more time, data resources, and more computational power to ensure proper training. A minor quantity of training samples might decrease the eminence of ML severely. ML in AI algorithms also helps in learning by dealing with massive quantities of data and discovering patterns impossible for detection otherwise [34, 35].

## 8 Impact of Neural Networks in Intelligent IoT

A neural network (NN) is a program algorithm that distinguishes the fundamental patterns and associations in a series of data with the help of a procedure very much comparable to ways that neurons and neural networks use in a human brain. NN, in

**Fig. 11** A Basic Unit (Neuron) in an ANN

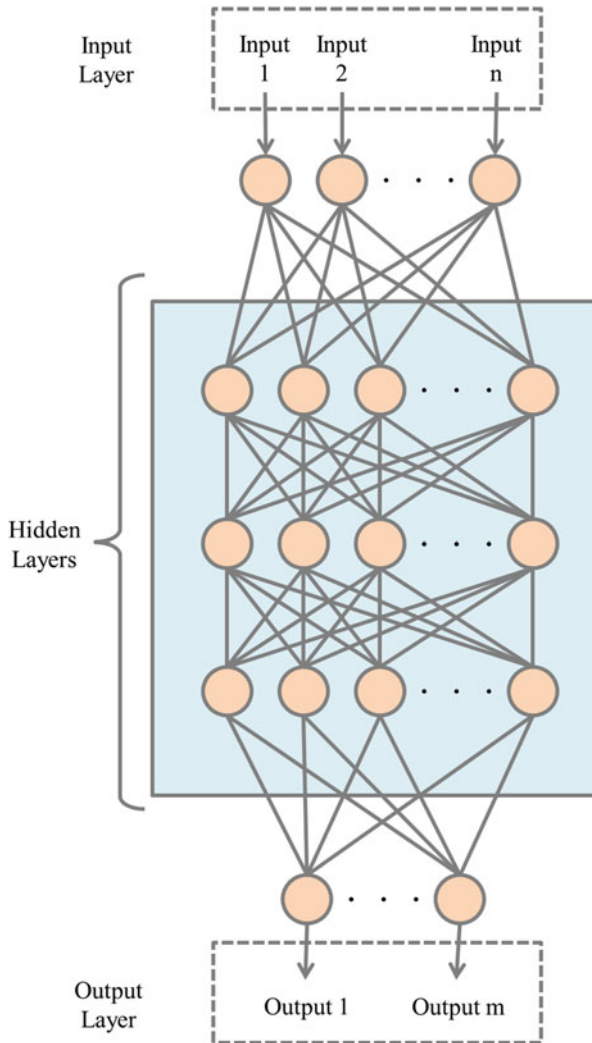


general, is defined as the system of neurons, which might be organic, while, in our case, it is artificial. Corresponding to this chapter, using the word “neural networks” refers to artificial neural networks (ANNs) only.

In an NN, the neuron is termed as the basic structure or building block, characterized by mathematical functions that categorize the data matching to a specific manner. NNs can adjust and update according to altering inputs, and thus the network creates optimal results without the need for continuously amending the output conditions (Fig. 11).

An NN typically contains layers of internally connected neurons. Often, a neuron is referred to as a node or a perceptron when defined corresponding to an NN. Each neuron usually has a basic structure of linear regression. The neuron first feeds the signals from numerous linear regressions on the way to an activation function that might even be nonlinear. ANNs are very useful in the expression of complex (nonlinear) functions. Additionally, they often learn these functions through the use of examples.

For multi-layered perceptron (MLP), neurons are structured in interconnected layers, creating a weblike arrangement. The first layer, referred to as the input layer, gathers input data. The intermediary layers, appropriately called hidden layers, define the input-to-output mapping of values. The final layer, also called the output layer, has groupings or output signals as results. Hidden layers frequently adjust input weightings iteratively until error gets minimized enough [36] (Fig. 12).



**Fig. 12** ANN Structure as a Multi-Layered Perceptron

NNs have successfully been applied to many real-world applications, which might be grouped into two classes: optimization and associative retrieval or classification.

For applications related to optimizations, the ANNs are utilized as state-space searching mechanisms. The synaptic weights have to be initially set before starting the searching process. There is generally no exact learning formula to decide the weights. Once synaptic weights are fixed, the recovering phase is achieved. The gradient descent has to be used in iterations until an optimal state convergence

is realized. Global optimal solution set can be found by utilizing the Boltzmann machine. With a proper schedule for annealing, the Boltzmann machine's state will progressively move toward the global optimal solution set [37].

Associative retrieval can be defined as the procedure of either recovering the pattern as a whole from the given partial set of information about the required pattern, that is, auto-association, or recovering patterns for a subset, analogous to patterns given in some other reference subset, that is, pattern association. The associative classification can be defined as identifying the associated category for some test pattern. A few learning schemes are occasionally used for these applications in training the synaptic weights [38].

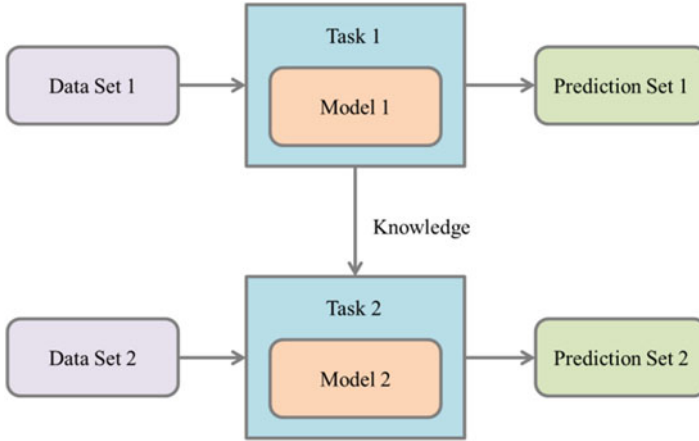
## ***8.1 Deep Learning***

Deep learning (DL) is a kind of ML that learns from unclassified or unlabeled data without any human being's tweaking or supervision requirement. It can handle enormous amounts of data that otherwise would take humans decades to understand and process. As such, DL is used for big data processing. The word "deep" denotes the presence of multiple layers in neural networks, having many nodes inside each layer, usually processing big data – data which is very big for storing volume. It is basically based on the notion that neurons found inside the human brain can comprehend abstract patterns and associations with the help of multiple neuron group layers [39].

DL utilizes a hierarchical level concerning ANNs for the implementation of ML process. The ANNs are organized much like a human brain, where neuron nodes interconnect much like the web structure. While the traditional algorithms tend to analyze data linearly, the hierarchical structure deployed in DL systems enables machines to function on data nonlinearly [40].

## ***8.2 Transfer Learning***

Transfer learning (TL) is another subset of ML whose primary focus is storing learned models while resolving one batch of data and applying that model to a correlated but separate dataset. For instance, an algorithm utilized to detect liver tumors may be utilized to detect brain tumors. Reusing or transferring information learned with previous models for the creation of newer models can tremendously improve the efficiency and speed of reinforcement learning agents [41] (Fig. 13).



**Fig. 13** Block Diagram of Transfer Learning

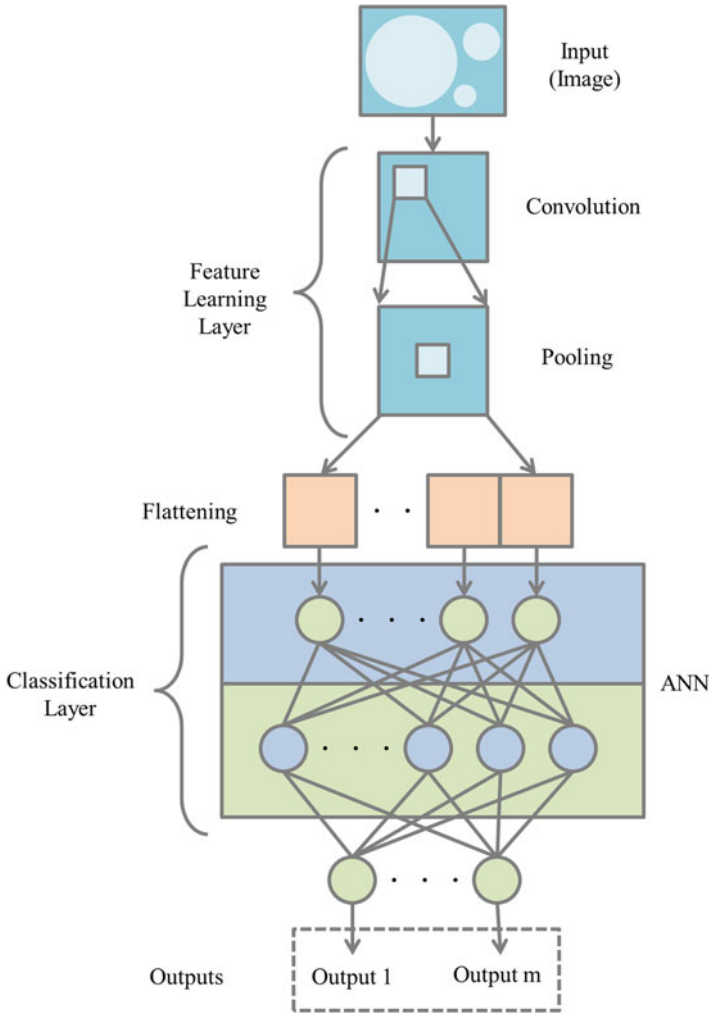
## 9 Convolutional Neural Networks for Intelligent IoT

A convolutional neural network (CNN or ConvNet) is an algorithm for DL which uses a multidimensional array as an input, such as the pixel values in an image, as set initial values, and then assigns changeable parameter values, called weights, to various constituents in the array, finally becoming capable for the differentiation of one from the other. In basic algorithms, filters are often placed manually, while CNNs learn these characteristics or filters over an operational range. The processing requirement of a CNN is considerably lower than most other classification algorithms [42].

A CNN commonly can discover and capture temporal and spatial dependencies effectively in images using necessary associative filters. The network can thus train to express the complexity for the image with better quality, as this algorithm performs much better fitting associated with the image dataset by reusing weights and reducing the involved parameters [43].

As the datasets grow in size for multiple dimensions, there is an exponential rise in the computational load. CNNs reduce the datasets to make them easier for computations, devoid of losses in the significant critical characteristics in getting a right prediction. The objective is an architecture design that excels at feature learning while scaled for enormous datasets. A CNN typically has two major components, a feature learning layer and a classification layer (Fig. 14).

The feature learning layer (FLL) is accountable for detecting and extracting both the low-level and high-level array features. The part in the multidimensional dataset taken for calculation purposes is termed a kernel. It can be one-dimensional or otherwise multidimensional itself, with many elements along each of the dimensions, but significantly lesser than the set of data that has to be processed. The kernel carries out the convolution for the first part of a convolutional layer [44].

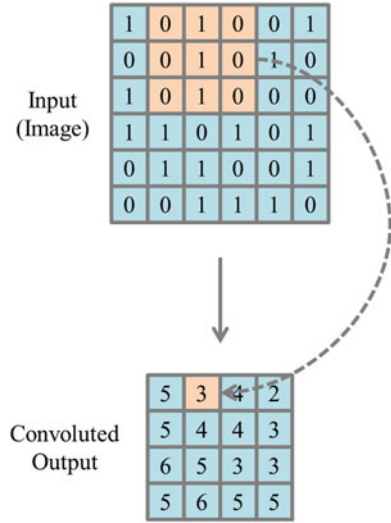


**Fig. 14** Block Diagram of a Convolutional Neural Network (CNN)

The kernel takes a specific dimension first. The first member of the associated dimension traces along a different dimension for each step until it parses the dimension completely. It then takes the second member and repeats the procedure. For greater than two dimensions, the other dimensions are nested just like the second dimension is for the first one. This procedure is continuous until the whole of the array; typically, an image gets traversed. Finally, all the results are summed with bias and provide us a convoluted feature output squashed to a one-dimensional channel [45] (Fig. 15).



**Fig. 15** Example of a Kernel Producing Convoluted Output



The convolution operation is extracting the high-level features for the input dataset, typically an image. CNNs may have one or multiple convolutional layers. Generally, the first of the convolution layers captures low-level features, for instance, edges and color. By the addition of multiple layers, the architecture adapts to get high-level features as well. Therefore, the structure now understands the dataset, much similar to how human beings perceive images. Convolution operation might produce two different types of results, namely, valid padding and same padding.

In valid padding, the convoluted result has a lower number of members in one or more dimensions for the array when compared to input. For instance, if valid padding is done on a (5x5x2) input array, the result might be an array with size (3x3x1).

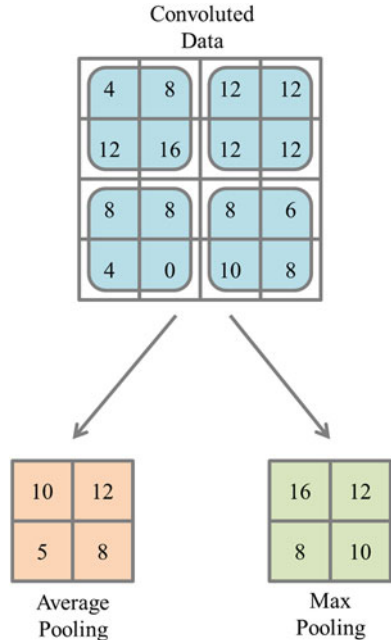
In same padding, dimensionality does not change, and hence its name. For instance, if same padding is utilized for a (5x5x2) input array, then the result also turns out to be an array of size (5x5x2) as well.

Similar in a sense to the convolutional layer (CL), the pooling layer (PL) also reduces the spatial size for convoluted result. The motive is to reduce the computations required to process the data using a reduction in the number of members or elements. It is also useful for the extraction of dominant features. It maintains the training procedure of the model efficiently. Pooling is of two types, namely, average pooling and max pooling.

The sum of all the values of a part of the image represented by the kernel is obtained using average pooling. It also employs spatial reduction as a noise reduction technique.

The maximum of portion of the image occupied by the kernel is obtained using max pooling. It also acts as a noise suppressant, as it filters out noisy activations

**Fig. 16** Average Pooling vs. Max Pooling



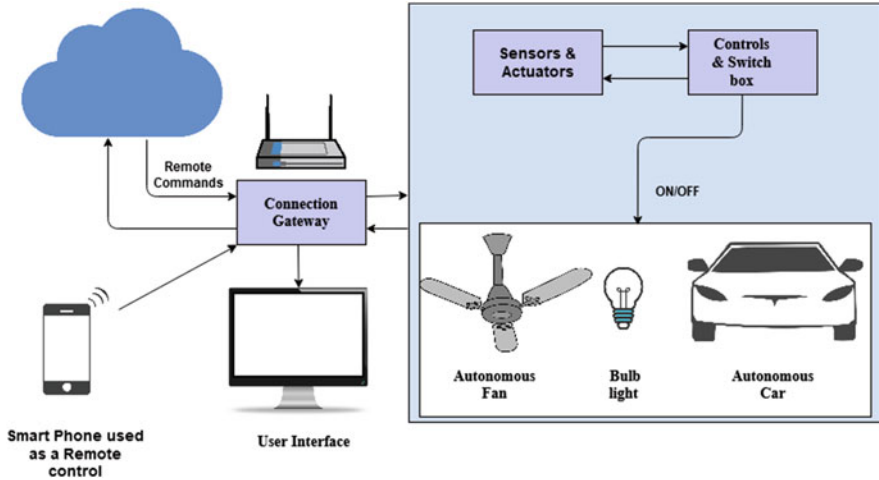
when denoising the image. When compared to average pooling, max pooling performs much better (Fig. 16).

The CL and PL cascaded together to form a feature learning layer entity. Depending on the problem complexity, a feature learning layer might as well have multiple convolutional-pooling pairs. The number of pairs increases with added complexity, and as a consequence, there is also an increase in the computational load.

After the feature learning stage gets finished, the resulting dataset passes through the classification layer stage, which consists of a regular ANN. The classification stage is only used after proper flattening to a single dimension. The ANN then takes care of the classification process [44, 46].

## 10 Recent Breakthroughs and Techniques

Applications of the Internet of Things have proven to be a revolutionary game-changer in industrial automation applications. Internet of Things (IoT) encapsulated with sensors and networks enables an option to connect with the Internet for transmitting data. Recent developments of IoT include home automation, industry applications, big data, etc. IoT has a tremendous impact on our lives in different ways with several perspectives. Implementing IoT in existing technologies helps us solve some severe real-world problems in healthcare units, smart home applications,



**Fig. 17** Different Kinds of Applications of IoT

smart industry automation, and smart wearable gadgets. Different unique applications of IoT in automation have been described as follows:

1. Applications in home automation – Home appliances such as tube lights, fans, and refrigerators could easily be controlled using IoT technologies. By accessing through IP address in an android smartphone, network connection establishes from a remote location. The speed of a fan and intensity of bulb light could easily be controlled and varied by using IoT. This application is efficient, auto configurable, secure, and remotely accessible [47].
2. Applications in industry automation – Deploying IoT in almost every industry is possible due to technological advancement. Smart networks connected to a cloud system could be used as an alternative to classical human-enforced tasks. For example, Tesla has introduced autonomous cars, capable of driving and navigating on their own without trained drivers.
3. Applications of IoT in advanced packaging – Tracking tools like road conditions, weather forecast, and other environmental circumstances could be justified and validated before transportation services using IoT. IoT is beneficial and can be used to track the damaged products/packages by business organizations.
4. Applications of IoT in security – By utilizing fire sensors, IoT could provide safety and security to indoor premises. It can continuously monitor all the safety measures and alerts in an emergency. IoT could also be used to track the status of injury in case of emergency (Fig. 17).

## 11 Intelligent IoT Reshaping Smartphone Applications

- AirSense [48] is the application used to monitor air quality both indoor and outdoor using smartphone sensor data of users. It takes input data from devices like wearable sensors but collects information via smartphone applications of users [49].
- NoiseSense [50] is an IoT-based smartphone application that is suitable for getting a noise pollution blueprint of the entire city by utilizing the microphone noise of each user's smartphone and maintaining privacy and security. It generally exploits the microphone's inbuilt sensor and monitors the noise data and transmits it to the cloud for further analysis. This system also provides individual noise exposure, suitable for personal health monitoring [51].
- An IoT-based smart classroom can increase the efficacy of the management, administrative council of a smart classroom. Radio-frequency identification (RFID) technology embedded with IoT helps identify and detect people and necessary objects. Other technologies, including Bluetooth, cloud networks, and Wi-Fi, can function similar applications with IoT. Applications such as fan speed and tube light are monitored using a smartphone or tab or even PC. RFID can automatically control the fan speed or tube light based on the current room temperature or classroom capacity [48].
- IoT-enabled healthcare systems could effectively restrain the spread and quick identification of various diseases [51]. The application is extremely beneficial for patients who require constant monitoring and observation in hospitals [52]. It also includes transmitting sensitive, essential data to the concerned doctors and hospitals through a smartphone.

## 12 Current Challenges and Future Opportunities

### 12.1 Challenges in Object Identification

Domain Name System (DNS) is used to translate domains to Internet users as IP addresses. However, DNS is susceptible to severe threats, including man-in-the-middle attack, UDP flood attack, TCP SYN flood attack, and cache poisoning attack. Domain Name Service Security Extension is used as a security extension of DNS. Its data integrity protection lets the receiver know about the data that has not been modified during transmission, although deploying it in IoT is still a challenging task for scientists and researchers. While transmitting data can cause delay and traffic congestion, thus, incorporating IoT is a challenging task [53].

## ***12.2 Privacy***

IoT deals with sensitive information like health data and personal information in healthcare applications [54]. IoT networks can be used to collect this information without the owner's consent; however, the majority of the networks keep the users informed about the data being monitored or administered. Current challenges include identifying the nodes capable of using or transmitting sensitive information passively through IoT networks [55].

## ***12.3 Evidence Collection and Preservation in Forensics***

Detection of IoT devices' existence in a forensic examination is quite demanding as IoT devices can work independently and maintain privacy [56]. Even if it gets detected, there is no reliable tool to verify evidence from the device. Real-time interaction between different nodes to preserve crime scenes is quite tricky in any IoT network [57].

## ***12.4 Future Challenges***

- An efficient, reliable, and secure IoT architecture is required to communicate with a large number of devices continuously, although it is a huge challenge to maintain its security and transmission efficacy altogether.
- The majority of IoT applications involve third-party interference for the smooth transmission of information between communicating devices. These third-party tools can manipulate or steal the sensitive information of users. Cryptographic solutions can be implemented with IoT devices due to their integrity and confidentiality characteristics [58].
- IoT can redefine healthcare applications to provide a more accurate, efficient result to its customers. IoT-enabled devices could be used for instant information response based upon user requirements. For instance, smart wearable devices could provide customized recommendations like suitable exercises and type of diet meals to be done after having an exhausting day [59].
- IoT in smart farming could be used as a new technique to help farmers make smart decisions by evaluating real-time weather data, air, and soil quality via smart sensors. This would assist the farmers in intelligent analysis and planning of harvesting and planting crops in the future [59].

## 13 Conclusion

Intelligent IoT is a versatile emerging technology that promises more reliable, efficient, and accurate IoT services. The capabilities offered by the use of AI in IoT result in intuitive thinking by the machines to leverage the automation industry to new heights. IIoT, even being a comparatively new paradigm, already finds applications in all walks of life, ranging from personal entertainment and hygiene, home and garage automation, and self-driving cars to large-scale projects such as revolutionizing farming, prevention of frauds, national security, and privacy, just to name a few. The AI component in Intelligent IoT is an emerging technology with new research and finding now and then. As AI's quality increases and IoT becomes increasingly accepted in the market, Intelligent IoT will continue to transform the way long-distance control and automation industry are working. In the future, shortcomings of present-day Intelligent IoT technology can be improved. For instance, privacy- and security-enhancing algorithms can be made better to detect ever-evolving fraudulent techniques, and ways to incorporate Intelligent IoT in the market may need attention. If developed on the right path, intelligent IoT proves to be an invaluable tool to eradicate the difficulties of today's problems. It will add an extra dimension to the comfortable future life of human beings.

## References

1. S. Nižetić, P. Šolić, D.L.D.I. González-de, L. Patrono, Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **274**, 122877 (2020)
2. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Commun. Surv. Tutor.* **22**(2), 1191–1221 (2020)
3. D. Evans, The internet of things how the next evolution of the internet is changing everything (April 2011). In *White Paper by Cisco Internet Business Solutions Group (IBSG)* (2012)
4. D. Basu, R. Datta, U. Ghosh, Softwarized Network Function Virtualization for 5G: Challenges and Opportunities. In *Internet of Things and Secure Smart Environments: Successes and Pitfalls* (2020), 147
5. U. Ghosh, D. B. Rawat, R. Datta, A.-S. K. Pathan (eds.), *Internet of Things and Secure Smart Environments: Successes and Pitfalls*, 1st edn. (CRC Press, 2020). <https://doi.org/10.1201/9780367276706>
6. Y.K. Chen, Challenges and opportunities of internet of things. In *17th Asia and South Pacific design automation conference* (IEEE, 2012), (pp. 383–388).
7. S.K. Singh, S. Rathore, J.H. Park, Block iot intelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. *Futur. Gener. Comput. Syst.* **110**, 721–743 (2020)
8. D. S. Sisodia, R. B. Pachori, L. Garg, eds. *Handbook of research on advancements of artificial intelligence in healthcare engineering*. (IGI Global, 2020)
9. C. Chakraborty, A. Banerjee, M. H. Kolekar, L. Garg, B. Chakraborty (eds.), *Internet of Things for Healthcare Technologies* (Springer, 2020)
10. N.A. Othman, I. Aydin, A new IoT combined body detection of people by using computer vision for security application. In *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)* (IEEE, 2017), (pp. 108–112).

11. V. Singhal, S.S. Jain, D. Anand, A. Singh, S. Verma, J.J.P.C. Rodrigues, N.Z. Jhanjhi, U. Ghosh, O. Jo, C. Iwendi, Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned Railway Level Crossings. *IEEE Access* **8**, 113790–113806 (2020)
12. P.K. Malik, R. Sharma, R. Singh, A. Gehlot, S.C. Satapathy, W.S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial internet of things and its applications in industry 4.0: state of the art. *Comput. Commun.* (2020)
13. I.B. Aris, R.K.Z. Sahbusdin, A.F.M. Amin, Impacts of IoT and big data to automotive industry. In *2015 10th Asian Control Conference (ASCC)* (IEEE, 2015), (pp. 1–5).
14. J. Chang, H.J. Liao, Y.D. Chih, M. Sinangil, Y.H. Chen, M. Clinton, S.L.L. Lu, Embedded memories for mobile, IoT, automotive and high performance computing. In *2017 Symposium on VLSI Technology* (IEEE, 2017), (pp. T26–T27).
15. S. Ghosh, S. Martin, S. Stelmach, Reliability for IoT and Automotive markets. In *2017 30th IEEE International System-on-Chip Conference (SOCC)* (IEEE, 2017), (pp. 1–3)
16. S. Stević, V. Lazić, M.Z. Bjelica N. Lukić, IoT-based software update proposal for next generation automotive middleware stacks. In *2018 IEEE 8th International Conference on Consumer Electronics-Berlin (ICCE-Berlin)* (IEEE, 2018), (pp. 1–4)
17. W.A. Ibrahim, M.M. Morcos, Artificial intelligence and advanced mathematical tools for power quality applications: a survey. *IEEE Trans. Power Deliv.* **17**(2), 668–673 (2002)
18. C. Ramos, J.C. Augusto, D. Shapiro, Ambient intelligence—The next step for artificial intelligence. *IEEE Intell. Syst.* **23**(2), 15–18 (2008)
19. J. Kozma, Intelligent agents. *IEEE Potentials* **17**(2), 16–19 (1998)
20. C.C. Lee, Fuzzy logic in control systems: Fuzzy logic controller. I. *IEEE Trans. Syst. Man Cybern.* **20**(2), 404–418 (1990)
21. J.M. Mendel, Fuzzy logic systems for engineering: a tutorial. *Proc. IEEE* **83**(3), 345–377 (1995)
22. X. Wu, Data mining: artificial intelligence in data analysis. In *Proceedings. IEEE/WIC/ACM International Conference on Intelligent Agent Technology, 2004.(IAT 2004)* (IEEE, 2004), (p. 7)
23. A.H. Sodhro, S. Pirbhulal, V.H.C. De Albuquerque, Artificial intelligence-driven mechanism for edge computing-based industrial applications. *IEEE Trans. Industr. Inform.* **15**(7), 4235–4243 (2019)
24. P. Chanda, S. Das, S. Banerjee, C. Chakraborty, Study on Edge Computing Using Machine Learning Approaches in IoT Framework. In *Green Computing and Predictive Analytics for Healthcare* (2020): 159
25. E. Alpaydin, Introduction to machine learning, 3rd (2014)
26. E. Mjolsness, D. DeCoste, Machine learning for science: state of the art and future prospects. *Science* **293**(5537), 2051–2055 (2001)
27. S. Bhattacharya, C. Chakraborty, Machine Learning for Biomedical and Health Informatics. In *Big Data, IoT, and Machine Learning: Tools and Applications* (2020): 79
28. P. Chanda, S. Das, S. Banerjee, C. Chakraborty, Study on Edge Computing Using Machine Learning Approaches in IoT Framework. In *Green Computing and Predictive Analytics for Healthcare* (2020): 159
29. D.L. Donoho, M. Elad, Optimally sparse representation in general (nonorthogonal) dictionaries via  $\ell_1$  minimization. *Proc. Natl. Acad. Sci.* **100**(5), 2197–2202 (2003)
30. K. Koh, S.J. Kim, S. Boyd, An interior-point method for large-scale  $\ell_1$ -regularized logistic regression. *J. Mach. Learn. Res.* **8**(Jul), 1519–1555 (2007)
31. K.P. Murphy, *Machine Learning: A Probabilistic Perspective* (MIT press, 2012)
32. M. Wu, B. Schölkopf, G. Bakır, N. Cristianini, A Direct Method for Building Sparse Kernel Learning Algorithms. *J. Mach. Learn. Res.* **7**(4) (2006)
33. G. Wang, M. Kalra, C.G. Orton, Machine learning will transform radiology significantly within the next 5 years. *Med. Phys.* **44**(6), 2041–2044 (2017)

34. J. Zhang, Z.H. Zhan, Y. Lin, N. Chen, Y.J. Gong, J.H. Zhong, H.S. Chung, Y. Li, Y.H. Shi, Evolutionary computation meets machine learning: a survey. *IEEE Comput. Intell. Mag.* **6**(4), 68–75 (2011)
35. G. Wang, J.C. Ye, K. Mueller, J.A. Fessler, Image reconstruction is a new frontier of machine learning. *IEEE Trans. Med. Imaging* **37**(6), 1289–1296 (2018)
36. B.K. Pathak, S. Srivastava, K. Srivastava, Neural network embedded multiobjective genetic algorithm to solve non-linear time-cost tradeoff problems of project scheduling (2008)
37. C. Lee, M. Gen, W. Kuo, Reliability optimization design using a hybridized genetic algorithm with a neural-network technique. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **84**(2), 627–637 (2001)
38. Y. Jin, B. Sendhoff, Reducing fitness evaluations using clustering techniques and neural network ensembles, in *Genetic and Evolutionary Computation Conference*, (Springer, Berlin, 2004), pp. 688–699
39. U. Ahmed, G. Srivastava, J.C.-W. Lin, A deep reinforcement learning model for data sanitization in IoT networks. *Comput. Netw.* **107914** (2021)
40. Z. Guo, K. Yu, L. Yu, G. Srivastava, J.C.-W. Lin, Deep Learning-Embedded Social Internet of Things for Ambiguity-Aware Social Recommendations. *IEEE Trans Netw Sci Eng* (2021)
41. L. Shao, F. Zhu, X. Li, Transfer learning for visual categorization: a survey. *IEEE Trans Neural Netw Learn Syst* **26**(5), 1019–1034 (2014)
42. A.A.M. Al-Saffar, H. Tao, M.A. Talab, Review of deep convolution neural network in image classification. In *2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)* (IEEE, 2017), (pp. 26–31)
43. G.E. Hinton, R.R. Salakhutdinov, Reducing the dimensionality of data with neural networks. *Science* **313**(5786), 504–507 (2006)
44. M.D. Zeiler, R. Fergus, Visualizing and understanding convolutional networks, in *European Conference on Computer Vision*, (Springer, Cham, 2014), pp. 818–833
45. C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke A. Rabinovich, Going deeper with convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (2015) (pp. 1–9)
46. K. Simonyan, A. Zisserman, Very deep convolutional networks for largescale image recognition, arXiv:1409.1556, (2014)
47. K. Simonyan, A. Zisserman, Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014)
48. J. Dutta, S. Roy, C. Chowdhury, Unified framework for IoT and smartphone based different smart city related applications. *Microsyst. Technol.* **25**(1), 83–96 (2019)
49. J. Dutta, F. Gazi, S. Roy, C. Chowdhury, AirSense: opportunistic crowd-sensing based air quality monitoring system for smart city. In *2016 IEEE SENSORS* (IEEE, 2016), (pp. 1–3)
50. J. Dutta, P. Pramanick, S. Roy, NoiseSense: crowdsourced context aware sensing for real time noise pollution monitoring of the city. In *2017 IEEE international conference on advanced networks and telecommunications systems (ANTS)* (IEEE, 2017), (pp. 1–6)
51. M. Walport, The Internet of Things: making the most of the Second Digital Revolution. *The Government Office for Science, UK* (2014)
52. Kulkarni A, Sathe S. Healthcare Applications of the Internet of Things: A Review. *Int. J. Comput. Sci. Inf. Technol. (IJCSIT)*. 2014;5(5):6229–6232. <https://doi.org/10.1.1.659.5696>
53. Z.K. Zhang, M.C.Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh, IoT security: ongoing challenges and research opportunities. In *2014 IEEE 7th international conference on service-oriented computing and applications* (IEEE, 2014), (pp. 230–234)
54. J. Lopez, R. Rios, F. Bao, G. Wang, Evolving Privacy: From Sensors to the Internet of Things. *Futur. Gener. Comput. Syst.* **75**, 46–57 (2017)
55. M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, K. Wehrle, A Comprehensive Approach to Privacy in the Cloud-Based Internet of Things. *Futur. Gener. Comput. Syst.* **56**, 701–718 (2016)



56. M. Harbawi, A. Varol, An improved digital evidence acquisition model for the Internet of Things forensic I: a theoretical framework. In *2017 5th International Symposium on Digital Forensic and Security (ISDFS)* (IEEE, 2017), (pp. 1–6)
57. M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things security and forensics: Challenges and opportunities (2018)
58. D. Sehwat, N.S. Gill, Internet of Things: Opportunities and Future Scope (2018)
59. B.S. Shruthi, K.B. Manasa, R. Lakshmi, Survey on Challenges and Future Scope of IoT in Healthcare and Agriculture. *Int. J. Comput. Sci. Mob. Comput.* **8**(1), 21–26 (2019)

# Smart Security for Industrial and Healthcare IoT Applications



M. Aruna, S. Ananda Kumar, B. Arthi, and Uttam Ghosh 

## 1 Introduction

Internet of Things (IoT) has paved the way for the rapid development of many areas which includes smart transport, smart city, smart home, smart healthcare, etc. Internet applications have become the order of the day, which has grown so rapidly and has become inevitable in almost all human activities [25]. IoT takes the help of various network devices to transfer and exchange data between physical objects which will be connected to each other. The main task of IoT thus becomes remotely regulating these objects throughout an existing network. The IoT device collects the information using the sensors associated with it and transfers it to the server after processing the data if required. The current trend of going for integration between the data processing systems for information and communication technology (ICT) and the medical fields (MF) shows a collective view of nerve connections outside the seam and devices that can improve healthcare services, and anticipate the advent of Internet of Things (IoT) healthcare. The population is growing, and aging is increasing. Diseases worldwide are seeking effective healthcare solutions protecting the health of the people. Another notable improvisation that has become

---

M. Aruna (✉) · B. Arthi

Department of Computer Science and Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Chennai, TN, India  
e-mail: [arunam@srmist.edu.in](mailto:arunam@srmist.edu.in); [arthib@srmist.edu.in](mailto:arthib@srmist.edu.in)

S. Ananda Kumar

School of Computer Science Engineering, VIT- University, Vellore, India  
e-mail: [s.anandakumar@vit.ac.in](mailto:s.anandakumar@vit.ac.in)

U. Ghosh

Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA  
e-mail: [uttam.ghosh@vanderbilt.edu](mailto:uttam.ghosh@vanderbilt.edu)

a development trend and gain widespread recognition around the world is the smart manufacturing system which is based on cyber-physical manufacturing system (CPMS). The primary advantage of IoT is to simplify human efforts, by intellectual techniques, which also makes inter-device connection smooth and effective in almost all the fields [22].

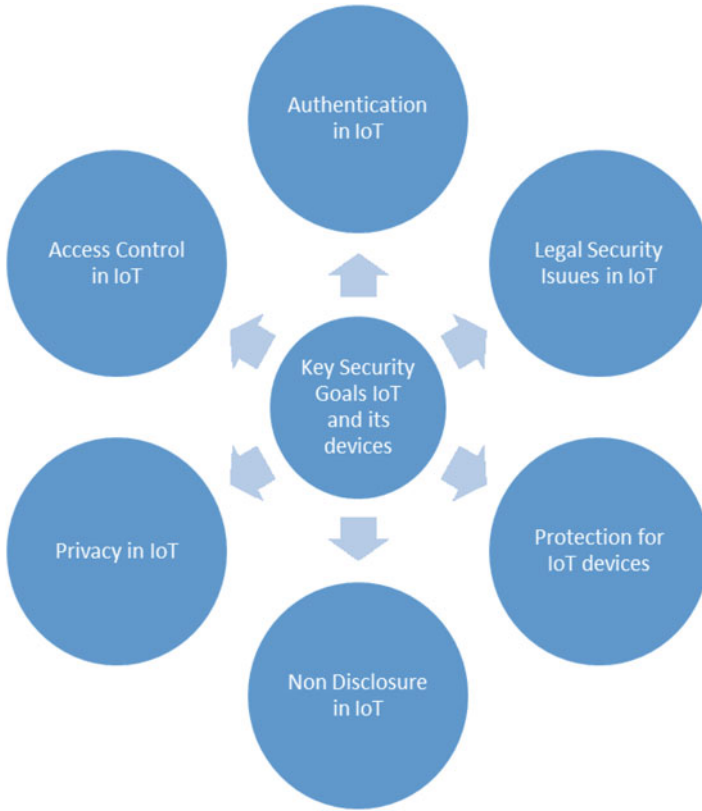
## 2 Key Security Goals in IoT

The advantages of IoT technology are many in number when we consider in terms of cost, effectiveness, efficiency, and ease of operation. Like any other advancement in science and technology, IoT also has its own drawbacks and disadvantages when misused. The major drawbacks identified in IoT integrated devices paves a way to many security threats, piracy, and data leaking and causes untold damage to the commercial, political, and social fabrics of a country.

The Internet of Things (IoT) is an inspiring field that combines intellect and intelligence to many essential functionalities of the modern-day world. IoT technology and its features are used in various sectors like homes, hospitals, cities, businesses, construction, and many more. One of the major limitations in the use of IoT and its applications or devices is the privacy and the security threats. This security issues are the main factors that is considered as the hindrance for the widespread use and acceptance of the IoT devices and applications. The storage and processing abilities of the IoT devices and their applications are usually constrained, and the design of these features currently focuses more on guaranteeing functionality and to a large extent ignores other conditions like the security and privacy issues (Fig. 1).

Majority of the security solutions that are currently available requires too many complicated computations and strategies, and hence they are expensive. The traditional security frameworks and algorithms that are currently available are actually very challenging to be implemented for many upcoming IoT devices and its applications or groups of IoT devices. IoT technology requires a flexible, adjustable, and reliable authentication and access control framework to take care of the security and privacy features of the IoT devices and their applications. The conventional access control model that has a centralized work structure cannot support the upcoming or evolving substantial and uncluttered IoT applications and devices. Hence, IoT requires a consistent, adaptable, and trustworthy access control methodology to certify the privacy and security aspects of trivial IoT devices. The traditional access control model has a centralized workflow and arrangement, and hence it is difficult for it to compliment the impending or progressing significant and uncluttered IoT applications and devices.

The lightweight certificateless signature (CLS) system includes niche and edge case scenarios in which there are four types of attacks of signature forgery that CLS fails to address. The first attack is called forgery attack based on public key replacement. Second in line attack is attack from a malicious-but-passive KGC. Third type of attack would be forgery attacks from anyone. The last type of attack



**Fig. 1** Key security goals in IoT

such a system is susceptible to is forgery attack from anyone based on any previous messages. Then the paper proposes a robust certificateless system (RCLS). There are several changes made in the generator functions to eliminate the possibility of the first three attacks. The fourth type of attack is eliminated by introducing a partial private key. To achieve higher efficiency, the RCLS scheme is based upon an elliptical curve analogue [18].

The rise of IoT as the fourth industrial revolution can provide a robust and scalable solution to support Industrial Internet of Things (IIoT) by decreasing the load of computational tasks from resource-starved machine-type devices (MTDs) to the high-powered edge servers. The problems of such a system would be the limited spectrum of resources, capacity-constrained batteries, and context unawareness. The proposed model is a learning-based channel selection model which takes into account the three distinct aspects of environmental awareness, namely, the energy consumption awareness, service reliability awareness, and the backlog awareness. The proposed algorithm SEC-MUCB outperforms the regular UCB algorithm by 13.7% and outperforms the range selection algorithm by 31.2%. The paper

concludes with the how MTDs can be utilized just for task offloading as they are fairly limited in their battery capacity. This is only achieved by the power edge computation [20].

### 3 Industrial Internet of Things (IIoT)

The myriad of trustworthy practices, issues and the application of such in IoT systems. The first point discussed is the idea of a unified IoT trustworthy environment establishment based on edge computing in Industrial IoT (IIoT). Here the threat level to the system depends on the number of IoT devices, and so it is hard if not impossible to counteract it. The machine learning algorithm models that are often trained on sensitive data usually leak the privacy to some form of adversarial attacks, thereby limiting the full potential in Industry 4.0. The work introduces a new approach called PriModChain, a framework that implements constraints for privacy and the trustworthiness on IIoT data by the amalgamation of differential privacy, federated ML, Ethereum blockchain, and smart contracts. The next group of articles discusses the trustworthiness of the system; here it starts with discussing how instrumental damages are done under different specific environmental conditions. Due to this, IIoT would essentially be able to detect system faults through environmental anomalies. The traditional security triad of confidentiality, integrity, and availability still applies to the IIoT, and now privacy must also be included. Finally, the last group of articles discusses the blockchain and its applications in vehicle connectivity [11].

The trustworthiness of a device in the Industrial Internet of Things (IIoT) network is an essential parameter expectation. Maintaining this trustworthiness as a recurring variable for every device in such a network is quite important to avoid loss. A device that is deemed trustworthy in an IIoT system combines the security characteristics of trustworthiness in the information technology sector, i.e., safety, privacy, reliability, security, and resilience. The Ensemble-learning method which combines random subspace (RS) with a random tree (RT) is used for detecting cyberattacks on any SCADA system by using the network traffics as a stream of data based on IIoT platform. A lack of availability of any other efficient and accurate security system for SCADA-based IIoT networks helps to bridge the gap as it satiates both scalability and reliability aspects which aren't present in the already existing systems [15].

With the combination of IoT technology and traditional M2M industry, the Industrial Internet of Things (IIoT) came into being which got the attention from all walks of life. With the increase in the number of IIoT devices in the networks of industrial environments, there is a radical need for research in securing IIoT systems from internal attacks; the threats to the security and quality of service (QoS) issues have skyrocketed. Internal attack is one of the important security issues that has made service environment unsafe and unreliable. Even though there is a lot of IIoT, there is no unified, standardized, and fine-grained system for trust evaluation to

handle the threats of internal attack and improve the overall QoS of IIoT. To this end, there is a need for a standardized model with a unified trustworthy environment which can be achieved by using edge computing which is being proposed; this system can detect malicious service providers and service consumers in a timely fashion, help filter fake data, and recommend the credible service providers. Edge computing is an effective service access point as it can support collection of service records to analyze and perform trust evaluations [17].

### ***3.1 Security Issues in IIoT***

Industrial Internet of Things (IIoT) applications aim at the automation industry. Industrial Internet of Things connects sensors, various instruments, and other devices that interact among each other and with computer that support industrial applications, which includes manufacturing, fabrication, and energy management. In the development trend of cyber-physical manufacturing system (CPMS), Industrial Internet of Things (IIoT) is a major issue [26]. Features like mechanization, automation, smart connect, real-time supervising, and cooperative control become the major issues for research and discussion [33].

There is a certain IoT-enabled health and access monitoring service questioning its customers about the location of different regions to optimize their travel in the geographical area. Elevated massive deployment costs of fully reliable information resources include IoT-enabled monitoring services sensing tools for citizen assignment and perhaps unreliable statistics collection for consumers. Nevertheless, trust management becomes a vital factor in the accomplishment of such facilities and services because they can mislead or delude customers through modification or counterfeiting. A hybrid unit or data trust calculation scheme was proposed for the monitoring service which depends on Bayesian practice to score data for users and the Dempster-Shafer theory (DST) for data fusion, only to calculate the reliability of the data. To provide flexibility against developmental change, the likelihood or probability mass used in the DST is updated vigorously relative to the user score above characteristics correlated with registered data [30].

One of the frameworks was proposed that measure the reliability of all data in the presence of on-off attacks. It was validated using massive simulation trials for uniform and on-off attacks. The trust scores differ under different system factors such as attack size and misdiagnosis. In addition, the reliability of all data can be measured using the utility theory and compared the results obtained by probability theory. The probability theory improves the reliability of all data compared to the correct utility theory [29].

The Social Internet of Things (SIoT) is an example of IoT devices that are networked, and they interact and evolve with each other. Social networks are interactions between them and their users. The influence of social relationships between devices and consumers depends on customers and their IoT services equipment. In this structure, evaluation of customer loyalty along with IoT devices is

necessary to prevent malevolent entities from spreading maliciously content or avoid the interruption of the network. One way to estimate companies the credibility for crowdsource companies is to deliver comment or feedback about the collaboration with certain IoT devices and users. Still, privacy protection in the form of crowdsourcing is a challenge as collaborative responses reveal communication devices and consumer behavior [32]. To deal with this issue, new privacy-protection system was proposed which assesses the reliability of IoT devices and users together in the SIoT ecosystem. This system implements a homomorphic encryption system which supports decentralization, self-implementation, and privacy protection. This ensures that the system is appropriate in computing, privacy, and consumer protection and detects the presence of malicious parties and a combination of consumers [31].

The Internet of Things is popular in all disciplines and in applications of smart construction, smart transport, health, and defense. One of the dimensions of IoT is the socialization of “things” called as Social Internet of Things (SIoT). There is a strong example that connects the principles of IoT and social networking, where the things involved are not only just autonomous and intelligent, but it also includes the social consciousness. A trust management plan was proposed to enable reliable automated decision-making built on the behaviors of objects. The popular SIoT trust metrics used are protection, significance, society interest, etc. Cooperative service scores are used to calculate the reliability power [27].

The distributive nature of IoT networks insists the need to design the appropriate security measures to assist in the detection of maleficent internal nodes. In earlier days the most extensive studies inferred that the attacks were considered primarily by single invasion, but the modern intruder may have more harmful effects since they perform multiple attacks simultaneously or in collaboration. One solution identified was using mix-attack models that have three types of attacks: attack, drop attack, and replay attack. A Distributed Consent Based Trust (DCONST) model was also proposed which utilizes both to assist in assessing the compliance of nodes and to identify bad IoT nodes and malicious individuals [28].

### **3.1.1 Security Issues in IIoT Based on Blockchain**

One of the major challenges in the Internet of Things (IoT) environment is maintaining data integrity and legitimacy of data sources. To guarantee data security, the conventional access control methods and frameworks that are available are not appropriate or adaptable for direct access control in IoT systems due to its complex access management schemes and absence of integrity. Hence, for secured and reliable IoT and IIoT, blockchain is one of the evolutionary approaches. It is a decentralized approach that aims at the security features of IIoT. Blockchain can be considered as a distributed ledger since all its blocks are chained together. It can track and coordinate transactions and save information for the billions of devices in the IoT. Blockchain is another important subject that is constantly evolving among the technology and the entrepreneurial society. Blockchain is a freely accessible,

visible, and distributed record that tracks all transactions between two groups very effectively which can be traceable, and which is permanent.

Blockchain is the primary security tool that is required for IoT systems. The combination of blockchain, fog computing, edge computing, and IoT devices are becoming extremely popular and useful. Incentive and feedback mechanisms are discussed as further enhancement for the system. The base blockchain is then compared to this enhanced blockchain where strength and weakness of both are compared in a tabular form. Then the author discusses wearable IoT devices; here the layers and the model for healthcare are discussed first, and then issues regarding security and privacy are discussed next. In AWS platform, the components of the API that enables IoT acts as a gateway for devices, message brokering, and rule operation engine. Finally the paper is concluded with referencing a suggestion made to AWSACIoT and the need for standardization in IoT's data collection and data sharing [2].

Blockchain technology acts as a framework for multimedia data processing. Its role is to ensure the privacy and transparency of any patient's records, ease of document accessibility and the shipment process among provider and customer. Blockchain phenomenon requires a web-based application consisting of two ends such as the front end that connects with the patients and a back end that facilitates patients to acquire the data from the blockchain. The miner's task here in blockchain is to provide proof of validation for correct task order. Even if the patient changes their doctor, the information regarding previous tests and medicines remain in the blockchain. The MAC layer protocol used is 802.11, and transmission ranges of MAP routers are 120 m/s. This type of system helps in computing the trust and rating of the nodes after a specific interval of time [10].

An efficient blockchain-assisted secure device authentication mechanism BASA IIoT is required to solve the problem of cross-domain internal communication among the IoT nodes while assessing and keeping the rising threat levels under check. Specifically, the consortium blockchain is primarily introduced to facilitate the construction of trust among several differential domains. The most exploited form of data authentication during the authentication process is identity-based signature (IBS); in order to preserve the privacy of devices, we need an identity management mechanism, which can comprehend that devices being authentic persist unknown. Besides, session keys between two parties are negotiated, which can secure the subsequent cross-domain internal communications. The limitations of BASA are the increased power consumption and the increase in communication overhead [12].

The differential privacy (DP) policy model achieves high records of privacy by maximizing the likelihood of the individual record identification. Other option is PriModChain; here there are two major components, namely, distributed entity (DISTEN) and central authority (CENTAUTH), which ensure the trustworthiness in terms of privacy, security, reliability, safety, and resilience of the IIoT system. DISTEN's task is to extract model parameters, whereas CENTAUTH applies multi-encryption key on the global parameters of the IPVC. Basically CENTAUTH first retrieves the encrypted IPFS hashes of the encrypted local (DISTEN) model



parameters that are released within the federation interval. PriModChain generates excellent results toward trustworthy privacy preserving in IIoT systems, and it reduces latency to improve efficiency [13].

The importance of Industrial Internet of Things (IIoT) lies in security as it is susceptible to a lot of single-point attacks and malicious attacks, which cannot in turn provide stable services. Due to the robustness and security brought by blockchain, this proposition about combining the security and stability of blockchain with the scalability of IoT has gained a considerable amount of traction. The major issue is that blockchains are power-intensive and low-throughput, making them unsuitable for a lot of power-constrained IoT devices. To combat these challenges, a blockchain system that is based on credit consensus mechanism for a network of IIoT devices is required. A credit-based proof-of-work (PoW) algorithm is the primary verification mechanism and a data authority management method for IIoT devices since it ensures security and transaction efficiency of the system at the same time and protects sensitive data confidentiality, which would regulate the accessibility to sensor data [16].

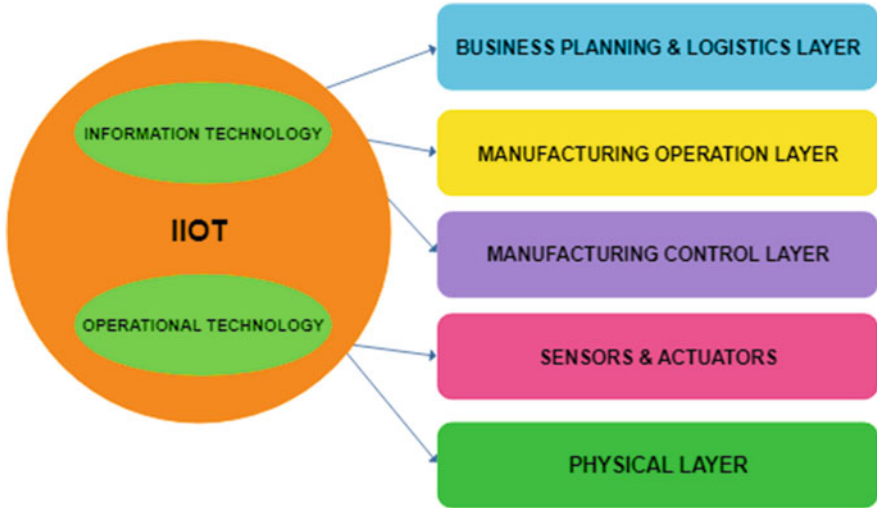
The fundamental problems affecting both IIoT and blockchain technology are interoperability, scalability, portability, and security. A platform-agnostic tokenizer for blockchain of IIoT devices referred to as Industrial Blockchain Tokenizer (IBT) helps with the tasks of data exchange in IIoT networks. This acquired data is then processed on a local system to get fruitful edge filtering results. This technology can bridge the gap between IoT and blockchain as well as result in standardization in both of them using IBT which can self-compute both cryptographic and networking operations leaving only the IIoT sensors and assets to do their job [19].

### 3.2 Industry 4.0

Industrial Internet of Things (IIoT) system is capable of realizing Industry 4.0 features of the industry that are normally assembled into operational and information technology (OT, IT) in order to promote technologies concepts, tools, and methods, which will enhance efficiency, flexibility, sustainability, and quality of life with reduced costs. Figure 2 shows Industry 4.0 architecture.

Each IIoT system and Industry 4.0 have the following requirement such as business, function, information, communication, integration, and asset concerns:

- Domain logic of the business is mapped to capture the grouped distribution of business across the IIoT device hierarchy and business logic and leads to understanding of the infrastructure and functional requirements of the business.
- To decompose the business capabilities into functional requirements using domain knowledge across the networked IIoT systems using service interfaces.
- The data, its meaning, and format are captured in information view.



**Fig. 2** Architecture of Industry 4.0

- Information passed between systems must be serialized/de-serialized, compressed/decompressed, and encrypted/decrypted and are captured using communications view.
- In integration view, hardware interfaces used in the systems for interacting with the physical world are captured.
- To identify the essential devices for running, the systems are captured in asset view since legacy devices are highly distributed in IIoT systems.

The system view can be used for development and estimation of the system and captures the asset, integration, communication, information, function, and business in terms of an implementation view. Table 1 shows various attacks and threats [9] [14] found in IIoT devices.

### 3.3 5G-Enabled IIoT

One revolutionary technology that is changing the appearance and work structure of the industries in a very smart way is the Industrial Internet of Things (IIoT). IIoT can be considered as one of the evolutionary applications in IoT in the field of industry and automation field. Although IIoT has many advantages and opportunities, it equally has many challenges and threats. IIoT connects sensors, actuators, computers, and many more that makes the manufacturing procedures extremely effective and smart. To accomplish the objective of “Internet of Everything (IoE),” cell network with wide inclusion has continuously become a strongly significant transporter of IIoT.

**Table 1** IIoT attacks and threats

	IIoT devices	Attacks	Threats
Operational technology	Sensors Actuators Motors Transmitters Embedded devices	<ul style="list-style-type: none"> <li>• Malware</li> <li>• Injecting input</li> <li>• Eavesdropping</li> <li>• Brute-force attacks</li> </ul>	<ul style="list-style-type: none"> <li>• Failure/malfunction of sensor/actuator</li> <li>• Device theft</li> <li>• Vandalism and sabotage</li> <li>• Man-in-the-middle attack</li> <li>• Session hijacking</li> </ul>
	Gateways Distributed control systems PLCs	<ul style="list-style-type: none"> <li>• Wireless device attacks</li> <li>• Replay attack</li> <li>• Man-in-the-middle attack</li> <li>• Sniffing</li> <li>• Brute-force password guessing</li> </ul>	<ul style="list-style-type: none"> <li>• Failure/malfunction of a control system</li> <li>• IoT communication protocol hijacking</li> <li>• Communication network outage</li> <li>• Network reconnaissance</li> <li>• Power supply outage</li> <li>• Loss of support services</li> </ul>
	SCADA control Operator stations Control room	<ul style="list-style-type: none"> <li>• Malwares</li> <li>• IP spoofing</li> <li>• Data sniffing and manipulation</li> </ul>	<ul style="list-style-type: none"> <li>• Unintentional change of data</li> <li>• Change in configuration of OT system</li> <li>• Erroneous use of devices</li> <li>• Maladministration systems</li> <li>• Third party's damage to system</li> </ul>
Information technology	Data centers Office application Web services	<ul style="list-style-type: none"> <li>• Web application attacks</li> <li>• Phishing</li> <li>• SQL injections</li> <li>• DNS poisoning</li> </ul>	<ul style="list-style-type: none"> <li>• Manipulation of hardware &amp; software, information</li> <li>• Denial of service</li> <li>• Malware and targeted attacks</li> <li>• Abuse of personal data</li> <li>• Brute-force attacks</li> </ul>
	Mobile devices Internet Business applications Data analytics	<ul style="list-style-type: none"> <li>• Mobile device attacks</li> <li>• DoS and man-in-the-middle attacks</li> <li>• Side-channel attacks</li> <li>• Authentication attacks</li> <li>• Cloud malware</li> <li>• Injection</li> </ul>	<ul style="list-style-type: none"> <li>• Failure or disruption of service providers</li> <li>• Failure to meet contractual requirements</li> <li>• Violation of rules and regulations</li> <li>• Breach of legislation</li> </ul>

The fifth-generation cell network (5G) which is happening is required to be a binding together organization that will associate billions of devices to help various business situations. But, as the industry needs, demands, and the number of the connected devices are growing tremendously, the conventional cloud-based IIoT framework is not efficient to handle it. The upcoming 5G era, which uses mobile edge computing (MEC) to improvise the 5G supporting IIoT, binds together organization that will associate many of devices to help various business situations. This type of architecture is normally data oriented. As indicated by the necessities of the IIoT application, the data structure and the data flow graph and the relating information structure are planned to start from the top.

Based on the fixed data plane, the information interaction is performed between the device and the application. It is easy to be implemented in small and simple

IoT requirements (e.g., smart homes). With the increase in the devices to be connected and the business requirements, the frame will not be suitable for an IIoT applications. With the advent of “Internet of Thing,” the cloud-based architecture requirement of IIoT is difficult to satisfy the requirements such as intensive computing, low latency, high reliability, and large connections. Considering this constrain, using MEC in IIoT applications has gained acceptance. However, it has been noted that mainstream MEC framework has limitation in providing the required support for the IIoT. Hence, a novel IIoT-MEC architectural framework was proposed which consists of three layers, namely, cloud computing layer, IIoT-MEC layer, and device layer.

In this new framework IIoT-MEC, the resource blocks in MEC servers are sliced into numerous resource blocks using Docker containers. Using the virtualization concept, the hardware details of the diverse IIoT devices are shielded using some resource blocks for device function virtualization. This simplifies the development of IIoT into a simple software development. With the resource block being used to support the IIoT operation services efficiently, a flexible object-oriented architecture is developed. The development of IIoT-MEC is done using Linux system, python language, and Docker container which makes the system highly compatible and minimizes the hardware requirement. This enables the IIoT-MEC to seamlessly integrate with any open-source platforms and work on low-cost machines like Raspberry Pi and PC.

## 4 IIoT in Healthcare

A unique framework model for the future IoT-based healthcare systems, which can be used for both standard programs and programs that assess specific situations, is proposed. Neutral sensors acts as a strong force on patient for recognizing important symptoms, blood pressure, and blood oxygen-levels. Communication rates are short and long; they are then compared according to appropriate healthcare applications. BLE and NB-IoT have emerged as the most appropriate standards of short width and long length in health, respectively. On analyzing some of the state-of-the-art tech in the new sensory fields, communication standards, and cloud technology, few key areas for some much-needed future research can be identified and analyzed. Machine learning and development of a secure systems are potentially strong in offering a solution to the researchers who want to make a big difference in IoT based health field [21].

The current trend of integrating the data processing systems for information and communication technology (ICT) and the medical fields (MF) shows a collective view of nerve connections outside the seam and devices that can help in improving healthcare services, and anticipating the advent of Internet of Things (IoT) healthcare. This provides relevant guidance for IoT health service developers, starting with the user’s view of technology. In particular, the authors suggest potential risks impact on users’ access to IoT lifecycle management service. Details on

professional service providers, scope of work, devices, professional support, and shared lists of personal medical information were suggested as important attributes. Friendship analysis is calculated by measuring the equal value of suggested symbols and service description options. The study can be performed by collecting the medical information and medical history from many respondents, analyzing the data and model, and then comparing the power groups with distinct medical history. The results have shown that the prospective users, basically, need a reliable, secured, harmless, and safe health service. This model has a great potential, while medical history has had a profound effect on what is known the significance of the proposed symbols.

As the population is rising enormously and the aging is increasing, diseases worldwide are seeking effective healthcare solutions protecting the health of the people. IoT healthcare monitoring applications can help reduce stress on healthcare systems and for healthcare providers, thus reducing and improving healthcare costs. Homecare and particularly elderly patients with persistent disease can be majorly benefitted from this. Healthcare sector and IoT Tiered Architecture (IoTTA) proposed a policy to change sensor data in real-time clinical responses. This methodology examines several features including sensing, sending, processing, storage, and mining learning. This framework is useful and aids in the development of effective steps to continue system enhancement in IoT healthcare applications. The growth of some IoT applications has huge implications for the healthcare industry as concerning to fields such as self-care, data mining, and machine learning [23].

Figure 3 depicts the various applications of IoT in healthcare. As the recognition of the Internet of Things (IoT) devices and additional remote patient monitoring systems increases, the security issues related to these devices also increase. About data transfer and logging of transactions, to maintain protected health information (PHI) blockchain-based smart contracts can be used to enable reliable analysis and maintenance of the medical sensor. To write the records of all events in the blockchain, a private blockchain which is based on an Ethereum protocol is used. This blockchain is used to build a system with sensors that communicate with a smart device called smart agreement. This smart agreement approach helps in medical field for real-time patient monitoring and medical intervention by sending reports to patients and medical experts, who also have a protected record of carrying out these activities. It helps fix the multiple issues with security and major real-time vulnerabilities associated with the use of remote patient examining and automatic distribution of information to all participated parties in a HIPAA-compliant manner [24].

The current IoT healthcare data integration semantic techniques include wearable body area network (WBAN), body area network (BAN), intelligent medical sensor (IMS), and personal monitoring device (PMD). The ontologies such as Resource Description Framework (RDF) and its schema are discussed. Then other technologies like Web Ontology Language (OWL) and semantic techniques like Simple Protocol and RDF Query Language (SPARQL) are also discussed. One of the techniques for data integration is clustering, and then distribution-based



**Fig. 3** Applications of IoT in healthcare

mechanisms are used, as being good with synthetic data that forms distinctly sized clusters but has a poor exception handling. The other technique is centroid based model which is fast and accurate, but moderately useless if the number of clusters is unknown or data is too large [1].

A new protocol for IoT healthcare communication, WBAN, is implanted in the body, and all the sensors are connected to a body coordinator (BC). This BC can be supplemented with external power unlike the sensor nodules. All the sensors are connected to this BC in star topology. Next, the paper discusses the traffic taxonomy, for example, emergency traffic, delay-constrained traffic, reliability-constrained traffic, and normal traffic. Then the ThMAC proposition is further lined. The primary component of this model is modeling thermal rise; here an equation is given to find out the temperature of point  $x,y$  as at any given time. A superframe is the second component to ThMAC; here beacon-enabled mode is followed. The next component is thermal-aware wake-up schedule; here the communication cycles of sensors within the superframe are discussed. Fourth component is the MAC operations carried out under ThMAC during a superframe; here contention access periods, polling periods, DL periods, CFP periods, and emergency data management are discussed. ThMAC is then tested in a simulated environment. This

is measured by maximum rise in temperature metric. The paper concludes with ThMAC outperforming IEEE 802.15.6 in achieving lower average temperatures and energy efficiency [3].

The fundamentals of IoT-based solutions in assisted ambient living (AAL), relies on the framework of semantic message-oriented middleware (SeMoM) architecture. After this the model being proposed is discussed; the discussion starts with laying down the methodology of the model. Any anomalies in the AAL system are traced and sent to a symptom indicator (SI); this stream of symptoms is then analyzed to figure out the disease. If multiple instances of similar disease are observed in close vicinity, an epidemic is detected. There is a SeMoM extension here added to the system. The ADL component is responsible for sensors and their ontology, SI component acts as a publisher of SI streams, and finally the disease component acts as a recipient of these streams from SI. A scalable semantic framework is proposed for disease and epidemic monitoring in a compound of elderly. This framework would have a significant effect in improving safety and aging in place for elderly as long as they desire staying at home. The power of this newly proposed system comes from the scalability and precision required to facilitate required results in detection of epidemics [4].

Figure 4 represents the various advantages of using IoT in healthcare applications. The security concern for user-generated data (UGD) is done through digital real-time consent which involves data collection for medical research. This is explored further, in which the data rights of the users is investigated deeper into the trust management aspect of IoT. Identification of trustworthy and untrustworthy parties is explored as well. The Health Insurance Portability and Accountability Act (HIPAA) is concerned about data privacy rights of the consumers, and data quality parameters include accuracy, authenticity, confidentiality, freshness, availability, and integrity. The basic three principles in the framework are the following: data should only be collected and used by trusted and certified entities with consent, data collection should be done in real time, and proper cryptographic mechanisms must be employed for the purpose of data protection. The privacy-preserving participants' selection methodology is required for user data consent and data monetization to encourage use participation. The framework combines all of the prior-mentioned components into one model for standardization in healthcare IoT [5].

IoT architecture of healthcare systems and its primary applications has a lot of challenges and also potential opportunities among which cloud integration and its components and the role of big data in IoT are considered primary. After establishing the components of IoT healthcare system, the shortcomings of each of these components are discussed. The first point of contention is as IoT devices are used all over the body and for extended period of time, the comfort levels of such devices need to be assessed. The next problem is that of noise removal in digital signal in real time. Removing human supervision with multiple agent machine learning algorithms checking, tracking, and determining the appropriate actions is not only cost-effective but also yields higher accuracy levels. The next point of contention is energy consumption and requirement of better energy optimization algorithms. The next problem mentioned is that of storage, where vast amounts of



**Fig. 4** Advantages of using of IoT in healthcare

data points are stored, but this storage needs to be easy access. Lastly the paper explores the area of privacy regarding IoT devices. The IoT healthcare architecture provides effective monitoring of the elderly patients by using a camera, speaker, and sensors that improves scalability and reliability [6].

Smart remote monitoring in real-time operations requires ease of access and transmittance of decisions based on acquiring data that includes data handling, data consent, data acquisition, and instrumentation and measurements. Due to the alteration of potential difference in cells, bio-signals such as ECG, EMG, EEG, and EOG are extremely low in amplitude. The signals that have such low amplitude can use bio-amplifiers, and that have low bandwidth and are prone to noise can use bio-compatible electrodes. Safety and isolation circuitry and special measurements are required since bio-signals are activated from different parts of the body. The procedures of data digitization, noise filtering, event identification, and extraction of data done in order to improve the interaction of various small and seemingly unrelated changes result in emergence of a healthcare system model where there is a vast integrated, ubiquitous, and holistic network that can be further supplemented [7].

The current ECG monitor system is low power, has higher processing speeds, and interfaces with multiple communication platforms, but the developed Telecare-ECG IoT device can be used to provide healthcare facilities to patient's home where the equipment can be operated even by nonspecialist users, with limited power supply sources, or used in industrial areas for out-of-hospital cardiac patients who operates daily for acquiring and processing of physiological parameters of the patients. There is a proposition for patients with highly optimized and specialized medical services [8].



## 5 Conclusion

A deep study on security issues in IoT, Industrial IoT, and its applications and the healthcare in IoT has been carried out. This chapter concludes with various security issues in IoT and IIoT and its applications and healthcare applications. The performance of security challenges is varying for the IoT-based applications. The extensive security issues are studied for IoT healthcare applications, and for industrial applications. This study focuses on the basic and emerging technology of IoT trust issues and various methods of Industrial IoT, Industry 4.0, and 5G-enabled IIoT also for various applications of IoT in healthcare. IoT will be creating a new generation of society enabled with information and knowledge. The application of IoT is unlimited due to advancement in technologies and the ease of integrating multiple devices and components, especially in the consumer sector where most of the homes appliances and systems are now integrated with the smart phones. This advancement has led to the requirement of different technologies to support such integrations. The future of IoT depends on having highly portable technologies which can work on different requirements.

## References

1. S. Balakrishna, M. Thirumaran, V.K. Solanki, IoT sensor data integration in healthcare using semantics and machine learning approaches, in *A Handbook of Internet of Things in Biomedical and Cyber-Physical System*, (Springer, Cham, 2020), pp. 275–300
2. M. Tawalbeh, M. Quwaidar, A.T. Lo'ai, Authorization model for IoT healthcare systems: Case study, in *2020 11th International Conference on Information and Communication Systems (ICICS)*, (IEEE, 2020), pp. 337–342
3. M.M. Monowar, M.O. Alassafi, On the Design of Thermal-Aware Duty-Cycle MAC protocol for IoT healthcare. *Sensors* **20**(5), 1243 (2020)
4. R. Zgheib, S. Kristiansen, E. Conchon, T. Plageman, V. Goebel, R. Bastide, A scalable semantic framework for IoT healthcare applications. *J. Ambient. Intell. Humaniz. Comput.*, 1–19 (2020)
5. M.J.M. Chowdhury, A. S. M. Kayes, P. Watters, P. Scolyer-Gray, A. Ng. Patient controlled, privacy preserving IoT healthcare data sharing framework. in *Proceedings of the 53rd Hawaii International Conference on System Sciences*. (2020)
6. S. Selvaraj, S. Sundaravaradhan, Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Appl. Sci.* **2**(1), 139 (2020)
7. A.S.M.S. Arefin, K.M.T. Nahiyani, M. Rabbani, The basics of healthcare IoT: Data acquisition, medical devices, instrumentations and measurements, in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, (Springer, Cham, 2020), pp. 1–37
8. I. Zagan, V.G. Găitan, A.-I. Petrariu, N. Iuga, A. Brezulianu, Design, fabrication, and testing of an IoT healthcare cardiac monitoring device. *Computers* **9**(1), 15 (2020)
9. V. Sklyar, V. Kharchenko, ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios. in *The 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, (Metz, France, 2019), pp. 1046–1049
10. G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimed. Tools Appl.*, 1–23 (2019)

11. M.Z.A. Bhuiyan, S.-Y. Kuo, J. Cao, G. Wang, Trustworthiness in industrial IoT systems and applications. *IEEE Trans. Industr Inform* (2020)
12. M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, D. Xiaojiang, M. Guizani, Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE J. Sel. Areas Commun.* **38**(5), 942–954 (2020)
13. P.C.M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, M. Atiquzzaman, A trustworthy privacy preserving framework for machine learning in industrial IoT systems. *IEEE Trans. Industr. Inform.* **16**(9), 6092–6102 (2020)
14. A.C. Panchal, V.M. Khadse, P.N. Mahalle Security issues in IIoT: a comprehensive survey of attacks on IIoT and its countermeasures. in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 124–130
15. M.M. Hassan, A. Gumaei, S. Huda, A. Almogren, Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model. *IEEE Trans. Industr Inform* **16**(9), 6154–6162 (2020)
16. J. Huang, L. Kong, G. Chen, M.-Y. Wu, L. Xue, P. Zeng, Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Trans. Industr. Inform.* **15**(6), 3680–3689 (2019)
17. T. Wang, W. Pan, S. Cai, Y. Ma, A. Liu, M. Xie, A unified trustworthy environment establishment based on edge computing in industrial IoT. *IEEE Trans. Industr Inform* **16**(9), 6083–6091 (2019)
18. Y. Zhang, R.H. Deng, Z. Dong, J. Li, P. Wu, J. Cao, Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. *IEEE Trans Industr Inform* **15**(9), 5099–5108 (2019)
19. D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi, L. Ricci, L. Rizzello, A Blockchain tokenizer for industrial IOT trustless applications. *Futur. Gener. Comput. Syst.* **105**, 432–445 (2020)
20. H. Liao, Z. Zhou, X.W. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, S.H. Ahmed, A.K. Bashir, Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT. *IEEE Internet Things J.* **7**(5), 4260–4277 (2019)
21. S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: technologies, challenges, and opportunities. *IEEE Access* **5**, 26521–26544 (2017)
22. S. Kim, S. Kim, User preference for an IoT healthcare application for lifestyle disease management. *Telecommun. Policy* **42**(4), 304–314 (2018)
23. H. H. Nguyen, F. Mirza, M. A. Naeem, M. Nguyen. A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback. in *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, (IEEE, 2017), pp. 257–262
24. K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **42**(7), 130 (2018)
25. B. Oryema, H.-S. Kim, W. Li, J.T. Park. Design and implementation of an interoperable messaging system for IoT healthcare services. in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, (IEEE, 2017), pp. 45–52
26. J. Cheng, W. Chen, F. Tao, C.-L. Lin, Industrial IoT in 5G environment towards smart manufacturing. *J. Ind. Inf. Integr.* **10**, 10–19 (2018)
27. A.M. Kowshalya, M.L. Valarmathi, Trust management for reliable decision making among social objects in the social Internet of things. *IET Netw* **6**(4), 75–80 (2017)
28. Z. Ma, L. Liang, W. Meng, Towards multiple-mix-attack detection via consensus-based trust management in IoT networks. *Comput. Secur.* **101898** (2020)
29. M. Salimitari, S. Bhattacharjee, M. Chatterjee, Y.P. Fallah, A Prospect theoretic approach for trust management in IoT networks under manipulation attacks. *ACM Trans. Sens. Netw. (TOSN)* **16**(3), 1–26 (2020)
30. B. Shayesteh, V. Hakami, A. Akbari, A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. *Int. J. Inf. Secur.* **19**(1), 93–110 (2020)

31. M.A. Azad, S. Bag, F. Hao, A. Shalaginov, Decentralized self-enforcing trust management system for social Internet of things. *IEEE Internet Things J.* 7(4), 2690–2703 (2020)
32. G. Srivastava, S. Muneeswari, R. Venkataraman, V. Kavitha, N. Parthiban, A review of the state of the art in business intelligence software. *Enterp. Inform. Syst.* (2021). <https://doi.org/10.1080/17517575.2021.1872107>
33. U. Ghosh, P. Chatterjee, R. Datta, A. Pathan, Secure Addressing Protocols for Mobile Ad hoc Networks. in *Security Analytics for Internet of Everything*, (CRC Press, Boca Raton, 2019)



**Dr. M. Aruna holds a Ph.D. degree** in the Faculty of Information and Communication Engineering from Anna University, Chennai, India. She has 15+ years of experience in teaching. Her area of interest includes artificial intelligence, machine learning, IoT, cloud computing, and software engineering. She has published several articles in various reputed journals. She has also published a book chapter in CRC Press. She is an active reviewer of various journals. She has presented papers in various national and international conferences and attended many workshops, seminars, and faculty development programs to be in track with the changing technology and teaching methodology. She is a member of various scientific and professional bodies.



**Dr. S. Anandakumar holds a Ph.D. degree** in the field of computer science from VIT University. He possesses one decade of experience in teaching and worked as project assistant in IIT Kharagpur. His areas of interest include QoS in wireless sensor networks, green computing, mobile computing, ad hoc networks, MANET, data mining, and IoT. He has published numerous articles in Scopus and SCI-indexed journals. He presented his articles in various national and international conferences and attended many faculty development programs in order to keep pace with changing teaching environment. He is a member of various scientific and professional bodies. Apart from teaching he is passionate about social services and rural development activities.



**Dr. B. Arthi holds a Ph.D. degree** in the field of computer science and engineering from Anna University. She has 15+ years of experience in teaching. Her areas of interest include software engineering, IoT, cloud computing, and green computing. She has published several articles in various reputed journals. She has also published a book chapter in CRC Press. She has presented papers in various national and international conferences and attended many workshops, seminars, and faculty development programs to be in track with the changing technology and teaching methodology. She is a member of various scientific and professional bodies. She has been awarded the IET Inspiring Young Teacher Award for the year 2016–2017 for the IET Chennai.



**Dr. Uttam Ghosh** joined Vanderbilt University as an assistant professor of the practice of electrical engineering and computer science in January 2018. He obtained his Ph.D. in electronics and electrical engineering from the Indian Institute of Technology Kharagpur, India, in 2013, and has postdoctoral experience at the University of Illinois in Urbana-Champaign, Fordham University, and Tennessee State University. His main research interests include cybersecurity, computer networks, wireless networks, information-centric networking, and software-defined networking. Dr. Ghosh is selected for Junior Faculty Teaching Fellow for 2018–2019 in Vanderbilt University. He is also serving as associate editor and reviewers of reputed journals and conferences. He is a senior member of the IEEE and member of Sigma Xi, AAAS, ASEE, and ACM.

# Index

## A

Aarogya Setu app, 2  
Accidental fittings, 155  
Acetylcholinesterase inhibitors, 161  
Activation function, 148  
Active feedback loop, 131  
Activities of daily living (ADL), 165  
AdaBoost classifiers, 210, 212  
Adaptive linear network (ADALINE), 157  
Adaptive model, 208  
Adaptive segmentation algorithm, 178  
Advanced Encryption Standard (AES), 46  
Advanced Research Projects Agency Network (ARPANET), 22  
Adverse drug reaction (ADR), 54  
AFFECTIVA, 69  
Affective computing, 67  
Age attribute, 210  
Alzheimer's disease, 161  
Amazon Web Service (AWS), 287  
Ambient assisted living (AAL), 52–53  
Ambulances, 91  
Anti-spam filters, 156  
Arduino ATmega328P AVR microcontroller, 108  
Arduino microcontroller ATmega328P 8-bit, 116  
Arduino Uno, 109–111, 195  
Artificial intelligence (AI), 2  
  assistive technology, 3  
  block diagram, 333  
  bridge between IoT and, 3  
  diagnostic accuracy, 3  
  expert system (ES), 334  
  fuzzy logic (FL) system, 334

  genetic algorithm, 334–335  
  monitoring patients, 3  
Attacker rider, 253  
ATTEMPT, 14  
Autism spectrum disorder and medical data  
  ABIDE dataset, 244  
  dataset and preprocessing, 248–249  
  feature selection, 242–243, 248  
  nature-inspired algorithms, 244–247  
  neuronal activity, 240–241  
  proposed reinforced rider optimization  
    algorithm, 253–254  
  rider optimization algorithm, 250–253  
  search techniques, 241–242  
  semi-wrapper for, 256–261  
  wrapper feature selection, 254–255  
  wrapper model, 255–256  
Automated human body temperature  
  monitoring devices, 92  
Automation, 226  
Autonomous vehicle driving, 280

## B

Bayesian networks (BNs), 147  
Behavioral analysis, 6  
Beta coronavirus, 83  
Big data, 95  
Big Data Analytics (BDA), 226  
Biomedical engineering, 146  
Biomedical engineering in CI  
  in cardiovascular disease diagnosis,  
    156–158  
  electroencephalogram signal analysis,  
    160–161

- Biomedical engineering in CI (*cont.*)
  - electromyography signals analysis, 158–160
  - gait and movement patterns, 161–162
- Biosignals, 67, 85
- Blockchain-based healthcare networks, 141
- Blockchain technology, 128–129, 193
  - application of, 133–135
  - challenges of, 135–137
  - framework for, 137–140
- Blood glucose levels, 56
- Blood pressure monitoring, 56
- Blood volume pulse (BVP), 69
- Bluetooth, 189, 190
  - low power (LE), 41, 42
  - protocols, 23
  - related blood pressure monitoring systems, 110
  - technology, 106, 110
  - wireless technologies, 94
- Body sensor networks (BSN), 85, 173, 175
- BoostEMD, 72
- Boosting, 204, 208, 209
- Broad reinforcement learning (BRL) model, 280
- Bypass rider, 251
  
- C**
- Centers for Disease Control (CDC), 88, 93–94
- Cerebral palsy (CP), 161
- Certificateless signature (CLS) system, 354
- Channel-aware routing protocol (CARP), 52
- Child Health Information (CHI), 54
- Climate change, 219
- Clinical Data Warehouse (CWD), 147
- Cloud data centers, 289
- Cloud service providers (CSPs), 287
- CoAP management interface (COMI), 39
- Cognitive processes, 68
- Communication protocols, 23, 171
- Community healthcare, 53
- Computational Intelligence (CI), 145
  - artificial neural network, 147–148
  - in biomedical engineering
    - in cardiovascular disease diagnosis, 156–158
    - electroencephalogram signal analysis, 160–161
    - electromyography signals analysis, 158–160
    - gait and movement patterns, 161–162
  - cardiovascular diseases, evaluation and categorization of, 165–166
  - challenges, 153
    - CI-based metrics, clinical applicability of, 153–154
    - machine learning, medical field, 154–155
    - regulatory impediments and quality control, 156
    - susceptibility to attacks and security-related challenges, 155–156
  - contemporaneous work and development of, 146–147
  - emerging IoMT-based optimized wearable technology, 165
  - evolutionary computing, 149–150
  - fuzzy systems, 148–149
  - IoMT, human-machine interfaces in, 163–164
  - machine learning, 151–152
  - medical industry, emotion classification in, 164–165
  - in medicine and bioinformatics, 152–153
  - prognostication and effective decision-making, leveraging social media healthcare for, 166–167
  - swarm intelligence, 150–151
- Computer-aided diagnosis (CAD), 147
- Confusion matrix, 75, 76, 213
- Connecting protocol, MQTT
  - applications, 36
  - benefits, 36
  - brokers, 33, 34
  - broking, 33, 34
  - current aspects, 36
  - limitations, 36
  - QoS, 35–36
  - structure, 33, 35
- Conserving electricity, 292
- Contagious diseases, 147
- Continua Health Alliance, 30, 31
- ContinuousCare, 90
- Convolutional neural network (CNN), 69
  - average pooling vs. max pooling, 345
  - block diagram, 343
  - feature learning layer (FLL), 342
  - kernel producing convoluted output, 343, 344
  - valid padding, 344
- Core data processing, 86
- Covariance, 75, 76
- “COVID-19 Gov PK mobile app,” 91
- COVID-19 pandemic, IoT
  - AI and machine learning, 84
  - ambulances, 91
  - applications of IoT to combat, 90, 91

automated human body temperature  
     monitoring devices, 92  
 body sensor networks, 85  
 challenges using IoT  
     big data, 95  
     confidentiality, 94–95  
     data mining techniques, 97, 98  
     data protection, 96  
     data sharing, 95  
     hackers and cyber offenders, 94  
     novelty procedure, 95  
     privacy issues, 97  
     security, 94  
     smart city, 96, 97  
 ContinuousCare, 90  
 “COVID-19 Gov PK mobile app,” 91  
 digital health innovations, 90  
 digital telehealth, 90  
 future research, 98  
 HealthArc, 90  
 Health Net Link, 90  
 IoMTs, 85–86  
 IoT-3D printing, 93  
 IoT-implemented medical care  
     management, 84, 86  
 IoT portal online, 88  
 major application, 88–89  
 m-health, 86  
 origin and spread, 83  
 personalized treatment, 89  
 radars, 85, 93, 95–97  
 RFID readers, 87–88  
 smart watches and fitness trackers,  
     92–93  
 supermarkets, 92  
 telemedicine, 90  
 ubiquitous communication, 87  
 user interface (UI), 93  
 ventilators, 93  
 virus circulation, 84  
 wearable IoT, 87  
 wearable sensors, 92  
 web-based monitoring platforms, 86  
 Cryptographic hardware, 156  
 Cryptographic hashing, 134  
 Cryptographic protocol. *see* Security protocol  
 Cutting-edge technology, 152  
 Cyberattacks, 132, 193  
 Cyber-physical manufacturing system  
     (CPMS), 354  
 Cyber-physical systems (CPS), 177  
 Cybersecurity, 311, 319  
 Cyber training, 176

**D**

DAG information question (DIO), 49  
 Dallas temperature sensor DS18B20, 114–115  
 Data feature vectors, 210  
 Datagram transport layer security (DTLS)  
     protocol, 39  
 Data mining software, 97, 98  
 Data protection, 96, 319, 320, 366  
 Dataset attributes, 211  
 Dataset shift, 154  
 Decentralization, 135  
 Decision tree, 273  
 Decryption, 139  
 DECT UEL protocol, 44  
 Deep learning, 3, 4, 13  
 Deep Q-learning (DQN), 275  
 Deep reinforcement learning, 280  
 Defuzzification, fuzzy systems, 149  
 Dempster-Shafer theory (DST), 357  
 Denoising approach, 70, 72  
 Destination-Oriented Directed Acyclic Graph  
     (DODAG), 49  
 DET curves, 217  
 Detection error trade-off analysis, 213  
 Device to device architecture, 26  
 Diabetes, 195  
     diabetes prediction algorithmic models,  
         205–207  
     gestational diabetes, 200  
     prevalence of, 200  
     type 1 diabetes, 199  
     type 2 diabetes, 199  
 Diabetic foot ulcers (DFU), 147  
 Differential privacy (DP) policy model, 359  
 Digital health innovations, 90  
 Digital telehealth, 90  
 Direct contact, 88, 93, 219  
 Discrete optimization, 247  
 Discrete wavelet transform (DWT), 69, 175  
 Distributed database management system  
     (DDBMS), 134  
 Distributed denial of service (DDoS) attacks,  
     281  
 Dynamic voltage frequency scaling (DVFS),  
     295–296

**E**

E-CARP, 52  
 Efficient Differentially Private Data Clustering  
     Scheme (EDPDCS), 177  
 Efficient resource management, 293  
 e-Health, 90, 107

- e-Health kit, 69
  - 802.11ah/Wi-Fi, 44–45
  - Electrocardiogram (ECG), 110
  - Electrocardiography (ECG), 70
  - Electrodermal activity (EDA), 70
  - Electroencephalogram (EEG), 152
  - Electromyography (EMG)
    - binary classification of emotional responses, 74, 75
    - classification error, 77
    - commercial EMG reading technologies, 69
    - confusion matrix, 75, 76
    - covariance features, 75, 76
    - data acquisition, 71–72
    - data preprocessing, 72
    - Demšar significance diagram, 78
    - DWT, 69
    - electrode placement, 71
    - emotion identification, 69
    - experimental protocol, 74, 75
    - face-to-face communication, 68
    - facial EMG, 68, 69, 71, 78
    - feature extraction and reduction, 72–73
    - five appraisal checks, 68
    - Friedman test, 77
    - F-score, 73, 75
    - GSR signals, 69
    - Kappa, 73, 75
    - K-nearest neighbor, 73, 75
    - OMG-Emotion dataset, 73, 74
    - sensor, 70, 71
    - SFRs, 68
    - stages for remote IoT-based emotion recognition, 70
    - SVM, 69
  - Electronic health records (EHR), 152, 155
  - Electronic wellness appointments, 93
  - Embedded context prediction (ECP), 55
  - Embedded gateway configuration (EGC), 55
  - Embedded solutions, 70
  - e-medicine, 219
  - Emotions, 68, 164
  - Empatica E4, 69
  - Empirical mode decomposition (EMD), 72
  - Encapsulating security payload (ESP), 37
  - Encoder-decoder structure, 178
  - Encryption, 139
  - Enhanced IoT-based array of sensors
    - abstract, 112–113
    - Bluetooth technology, 106
    - circuit design proposed, 116–117
    - comparison table, 121–122
    - dallas temperature sensor DS18B20, 114–115
    - data explosion and high expectations, 106
    - end-user healthcare applications, 107
    - ESP8266-1 Wi-Fi module, 115
    - health vitals, 120
    - heartbeat sensor, 111, 114
    - IoT patient health monitoring system,
      - related studies on, 108–111
    - liquid crystal display, 115
    - microcontroller unit, 116
    - outputs, 119
    - proposed system, 114, 122
    - pulse sensor, 111
    - research and business, 108
    - ThingSpeak cloud, patient data stored on, 121
    - ThingSpeak web application, 119
    - ultraviolet detection sensor, 115
    - web application, 117–119
    - Zigbee module, 106
  - ENISA's baseline recommendation, 318–319
  - Entity authentication protocols, 24
  - Epilepsy, 160
  - ESP8266-1 Wi-Fi module, 115
  - e-storage, 2
  - Evolutionary algorithm (EA), 149, 245
  - Extensible authentication protocol (EAP), 40
- F**
- Facial EMG, 68, 69, 71, 78
  - False data injection (FDI) attacks, 281
  - Fast array of wimpy nodes (FAWN), 296
  - Feed-forward neural network (FFNN), 176
  - Fever monitors, 94
  - File transfer protocol (FTP), 23
  - Fisher's linear discriminant (FLD) method, 161
  - Fitness trackers, 93
  - 5G, 45–46, 196
  - Flash, 74
  - Flood sensor data, 280
  - Fog-access points (F-APs), 277
  - Fog computing, 201, 213
  - Fog computing, healthcare, 200
    - cost reduction, 203
    - equipment and drug management, 203
    - faster diagnosis, 203
    - fog healthcare-based architecture, 202
    - for hospitals, 202
    - improved treatment, 203
    - with patient's overall satisfaction, 203
    - for physicians, 202
    - proactive treatment, 203
    - reduction of errors, 203
  - Follower rider, 251–252



- Friedman test, 77  
 F-score, 73, 75  
 Function-as-a-Service (FaaS), 288  
 Fuzzification, fuzzy systems, 149  
 Fuzzy logic techniques, 159
- G**
- Gadget to gateway architecture, 25–26  
 Gait, 161–162  
 Galvanic skin response (GSR) signals, 69  
 Gateway to information frameworks, 26–27  
 Gaussian radial basis function, 166  
 GB classifiers, 210  
 Generic Attribute Profile (GATT), 41  
 Genetic algorithms (GA), 150, 157, 161  
 GENI-dependent networking technologies, 176  
 Genomic medicine, 153  
 Gestational diabetes, 200  
 Global warming, 219  
 GoDaddy, 287  
 Google Cloud Platform, 287  
 Green cloud computing
  - access control and least privilege, 299
  - advantages of, 292–293
  - applications of, 291–292
  - dynamic voltage frequency scaling (DVFS), 295–296
  - encryption in Cloud, 300
  - energy efficiency, 290
  - energy-efficient data center, 291
  - fast array of wimpy nodes (FAWN), 296
  - geographical location and data center cooling, 298
  - lateral spreading of attacks, 299
  - less control, 299
  - loss/theft of intellectual property, 298
  - minimal visibility, 299
  - multi-factor authentication (MFA), 300–301
  - nano data centers (NaDa), 296
  - penetration tests, 300
  - regulatory compliance violations, 298–299
  - shortcoming of, 293–294
  - SSH and Securely Store Keys, 300
  - thermal/heat management, 291
  - virtualization and VM consolidation, 296–297
- G.9959 system, 40–41
- H**
- HealthArc, 90  
 Healthcare systems, IIOT
  - advantages, 367
  - applications of, 365
  - data integration semantic techniques, 364
  - ECG monitor system, 367
  - friendship analysis, 364
  - monitoring applications, 364
  - neutral sensors, 363
  - protected health information (PHI), 364
  - SeMoM architecture, 366
  - smart remote monitoring, 367
  - ThMAC proposition, 365
  - user-generated data (UGD), 366
  - WBAN, 365
- Healthcare technologies, 179  
 Health Insurance Portability and Accountability Act (HIPAA), 366  
 Health monitoring systems, 105  
 Health Net Link, 90  
 Health services, 201  
 Heartbeat sensor, 111, 114  
 Helsinki Declaration, 74  
 Hidden Markov models, 157  
 Highway Addressable Remote Transducer (HART), 47  
 Huanan Seafood Market, 83  
 Human-computer interaction (HCI), 67  
 Human emotion recognition, 69
- I**
- IBM Cloud, 287  
 IEEE 802.16 (WiMAX), 46–47  
 Immutability, 135, 136  
 Indirect emergency healthcare (IEH), 55  
 Industrial Internet of Things (IIoT)
  - attacks and threats, 362
  - 5G enabled, 361–363
  - healthcare systems
    - advantages, 367
    - applications of, 365
    - data integration semantic techniques, 364
    - ECG monitor system, 367
    - friendship analysis, 364
    - monitoring applications, 364
    - neutral sensors, 363
    - protected health information (PHI), 364
    - SeMoM architecture, 366
    - smart remote monitoring, 367
    - ThMAC proposition, 365
    - user-generated data (UGD), 366
    - WBAN, 365

- Industrial Internet of Things (IIoT) (*cont.*)
  - Industry 4.0, 360–361
  - PriModChain, 356
  - quality of service (QoS) issues, 356
  - SCADA system, 356
  - security issues
    - AWSACIoT, 359
    - blockchain, 358–360
    - Dempster-Shafer theory (DST), 357
    - differential privacy (DP) policy model, 359
    - distributive nature, 358
    - identity-based signature (IBS), 359
    - Social Internet of Things (SIoT), 357, 358
- Industrial, scientific, and medical (ISM) band, 189
- Inference engine, fuzzy systems, 149
- Information and communication technology (ICT), 90
- Information exchange, 140
- Infrared Data Association (IrDA), 190
- Infrastructure-as-a-Service (IaaS), 287, 288
- Instant messaging, 23
- Intelligent IoT system
  - artificial intelligence (AI)
    - block diagram, 333
    - expert system (ES), 334
    - fuzzy logic (FL) system, 334
    - genetic algorithm, 334–335
  - automotive industry, 332
  - breakthroughs and techniques, 345–346
  - comprehensive applications
    - better lifestyle, 330
    - improve healthcare, 330–331
    - personalized experiences, 331
    - save time and resources, 330
  - computer vision, 331–332
  - concept of, 329
  - convolutional neural network (CNN)
    - average pooling vs. max pooling, 345
    - block diagram, 343
    - feature learning layer (FLL), 342
    - kernel producing convoluted output, 343, 344
    - valid padding, 344
  - dynamic flexibility, 328
  - evidence collection, 348
  - forensic examination, 348
  - future challenges, 348
  - image processing, 331–332
  - machine learning (ML)
    - block diagram, 336
    - reinforcement ML algorithm, 337, 338
    - semi-supervised ML algorithm, 337, 338
    - supervised ML algorithm, 336
    - unsupervised ML algorithm, 337
- neural network (NN)
  - artificial neural networks (ANNs), 339
  - deep learning, 341
  - multi-layered perceptron (MLP), 339, 340
  - synaptic weights, 340
  - transfer learning, 341–342
- object identification challenges, 347
- pattern recognition, 331–332
- privacy, 348
- reshaping smartphone applications, 347
- user-friendly products, 328
- International Telecommunication Union (ITU), 22
- Internet of Medical Smart Things (IoMST), 176–177
- Internet of Medical Things (IoMT), 145, 147, 171–172, 190
  - adaptive segmentation algorithm, 178
  - body sensor network, 175
  - challenges for, 180
  - communication system, 172–173
  - current approach, proposed solutions for, 180–183
  - cyber training, 176
  - Efficient Differentially Private Data Clustering Scheme, 177
  - encoder-decoder structure, 178
  - feed-forward neural network, 176
  - GENI-dependent networking technologies, 176
  - human-machine interfaces in, 163–164
  - Internet of Medical Things Security Assessment Framework, 176
  - risks of, 173–174
  - studies, 174–170
  - validation and verification, 177
- Internet of Medical Things Security Assessment Framework, 176
- Internet of Things (IoT), 105
  - applications, 10, 11
  - authorization model, 310
  - behavioral analysis, 6
  - big data applications, 222
  - comparative analysis, 14–16
  - computer-aided design, 6
  - database, 6
  - deep learning, 13
  - device protection, 311
  - device vulnerability exposure, 312

- 3D printing, 93
  - five-layer architecture, 270–271
  - fog-based healthcare innovations, 201
  - fog-based IoT architecture, 271
  - four stages of IoT solutions, 7
  - future directions, 14, 17
  - green IoT, 223
  - healthcare building, 308
  - human input, 5
  - improvement, 4
  - information and communication technology (ICT), 353
  - information integration, 6
  - infrastructure as a service (IaaS), 268
  - Internet of Medical Things, 7–8
  - knowledge base software, 6
  - machine learning, 11–13
    - in computing and resource management, 277–279
    - in decision making, 279–280
    - reinforcement learning, 274–275
    - security, 281–282
    - for Smart City scenario, 276–277
    - supervised learning, 271–274
    - unsupervised learning, 274
  - machine-type devices (MTDs), 355
  - medical and healthcare data, 200
  - medical lays, 307–308
  - need in healthcare devices
    - for health center, 9
    - for health insurance companies, 9
    - for medical experts, 9
    - for patients, 9
  - optimization techniques, 13–14
  - platform as a service (PaaS), 268
  - privacy and security, 310
  - problem sectors and probable IoT-based solutions, 222
  - QoS parameters, 223
  - resource optimization methods, 6
  - security goals, 354–356
  - sensor-tagged IoT devices, 202
  - smart sustainable city
    - smart farming, 231–232
    - smart healthcare, 232–233
    - smart transportation, 229–231
  - software as a service (SaaS), 268
  - strategic planning, 6
  - subsystem optimization, 6
  - sustainable IoT architecture, 224–225
  - sustainable smart cities, 222
  - three-layer architecture, 269–270
  - visualization interface, 5
  - wearable devices, 139
  - Internet protocol (IP), 23, 28
  - Internet Protocol Support Profile (IPSP), 42
  - Intrinsic mode functions (IMFs), 72
  - Intrusion detection system (IDS), 282
  - IPv6, 30, 31
    - 802.11ah/Wi-Fi, 44–45
    - bluetooth low energy, 41–42
    - DECT/ULE, 44
    - G.9959 systems, 40–41
    - MS/TP (6LoBAC), 43
    - NFC, 42–43
  - ISA 100.11a, 47–48
  - Isolation, 88, 92, 93, 96, 97, 232
- J**
- JavaScript, 74
- K**
- Kappa, 73, 75
  - K-healthcare, 178
  - K-Means clustering, 274
  - K-nearest neighbor (KNN) classifier, 73, 210, 273
  - Knowledge base software, 6
- L**
- LabVIEW, 108, 109
  - LED, 111
  - Likelihood ratio method (LRM), 161
  - Linear regression, 272
  - Link aggregation, 24
  - Liquid crystal display (LCD), 115
  - Local area networks (LAN), 22
  - Lockdown, 84, 219, 220, 227–229
  - Logical link control and adaptation protocol (L2CAP), 41
  - Logical link management (LLC), 38
  - Logistic regression, 273
  - LoRaWAN<sup>®</sup> Specification v1.1, 48
  - Low-power and lossy network IoT
    - adverse drug reaction, 54
    - ambient assisted living, 52–53
    - child health information, 54
    - community healthcare, 53
    - embedded context prediction, 55
    - embedded gateway configuration, 55
    - indirect emergency healthcare, 55
    - m-health, 54
    - semantic medical access, 55
    - wearable device access, 54

**M**

Machine learning (ML), 11–13, 204, 269  
 bias based on, 155  
 block diagram, 336  
 computational intelligence, 151–152,  
 154–155  
 reinforcement ML algorithm, 337, 338  
 semi-supervised ML algorithm, 337, 338  
 supervised ML algorithm, 336  
 vs. traditional programming approach, 309  
 unsupervised ML algorithm, 337

Machine-to-machine communication, 21, 86

Magnetic resonance imaging (MRI), 147, 154

Malicious behavior analysis, 140

Master-slave/token-passing (MS/TP)-based  
 protocol, 43

MATLAB software, 74

McKinsey Global Institute, 98

McNemar test, 73

Medical care insurance, 89

Medical decision systems, 159

Medical implant communication service  
 (MICS), 190

Medication management, 57

Medicine 4.0, 61

Medium access control (MAC), 38

Merkle tree, 310

Message queuing telemetry transport (MQTT)  
 applications, 36  
 benefits, 36  
 brokers, 33, 34  
 broking, 33, 34  
 current aspects, 36  
 limitations, 36  
 QoS, 35–36  
 structure, 33, 35

Metabolic disease, 199

m-health, 54, 107, 194

Microcontroller (MCU), 115

Microcontroller-based patient health  
 monitoring system, 109

Microcontroller unit, 116

Microsoft Azure, 287

Microsoft Band 3, 69

Middle East respiratory syndrome (MERS), 83

Miners, 134

Minimum toe clearance (MTC), 162

MIT-BIH database, 158

MLP-NN, 161

Mobile health (m-health), 54, 86, 107, 281,  
 282

Moisture sensor-operating facial masks, 97

MoodScope, 165

Movement patterns, 161–162

Multi-factor authentication (MFA), 300–301

Multilayer perceptron (MLP), 210

Multi-objective optimization, 247

MySignals, 70, 71

**N**

Naive bayes (NB) classifier, 273

Nano data centers (NaDa), 296

Near-field communication (NFC), 42–43

Nemenyi post hoc test, 77

Network encapsulation protocols  
 5G, 45–46  
 HART, 47  
 IEEE 802.16 (WiMAX), 46–47  
 IPv6 over  
 802.11ah/Wi-Fi, 44–45  
 bluetooth low energy, 41–42  
 DECT/ULE, 44  
 G.9959 systems, 40–41  
 MS/TP (6LoBAC), 43  
 NFC, 42–43  
 ISA 100.11a, 47–48  
 LoRaWAN<sup>®</sup> Specification v1.1, 48  
 6Lo-IPv6 (6Lo) working group, 40  
 6LoWPAN, 37  
 6TiSCH, 38–39  
 Zigbee, 39–40

Network management protocols, 23–24

Network protocol  
 categorization IoT protocols, 24, 25  
 communication, 23  
 connecting protocol (*see* Connecting  
 protocol, IoT)  
 encapsulation protocols (*see* Network  
 encapsulation protocols)  
 healthcare network architecture  
 Continua Health Alliance, 30, 31  
 IPv6, 30, 31  
 portability arrangement, 30–31  
 6LoWLAN layer structure, 30  
 vehicle-to-infrastructure (V2I)  
 communications, 31, 32

IoT healthcare networks  
 device to device architecture, 26  
 gadget to gateway architecture, 26  
 gateway to information frameworks, 26,  
 27  
 IoT system architecture, 26

LAN/WAN, 22

networking platform  
 automation design methodology, 34  
 health information service model  
 functional framework, 33  
 VRTUS, 32

- network management, 23–24
  - network topology
    - in healthcare portal, 29
    - multiple sensor data, 27
    - in role of portal, 29
    - TinyOS, 28
    - WiMAX combination, 28
  - telemedicine, 30
  - Network protocols
    - IoT healthcare applications
      - blood glucose levels, 56
      - blood pressure monitoring, 56
      - electrocardiogram monitoring, 56
      - medication management, 57
      - oxygen saturation monitoring, 56
      - rehabilitation systems, 57
      - smartphones, 57
      - wheelchair management, 57
    - IoT healthcare security
      - authentication, 58
      - authorization, 59
      - confidentiality, 58
      - error limitations, 59
      - information freshness, 58
      - integrity, 58
      - non-repudiation, 58
      - resiliency, 59
      - self-protection, 59
    - low-power and lossy network IoT (*see* Low-power and lossy network IoT)
    - routing protocols (*see* Routing protocols)
    - security challenges
      - computational limitations, 59
      - data privacy and security updates, 61
      - dynamic network topology, 60
      - dynamism, 60
      - energy limitations, 59
      - future aspects, 61
      - multiplicity of devices, 60
      - multi-protocol network, 60
      - scalability, 60
  - Neural Impulse Actuator (NIA), 69
  - Neural network (NN)
    - artificial neural networks (ANNs), 339
    - deep learning, 341
    - multi-layered perceptron (MLP), 339, 340
    - synaptic weights, 340
    - transfer learning, 341–342
  - Neural networks, 162
  - Non-line-of-sight (NLoS) network, 46
  - Non-wearable sensors, 174
  - NVISO, 69
- O**
- OCZ Technology, 69
  - OLAP application, 178
  - One-Minute Gradual-Emotional Behavior dataset (OMG-Emotion dataset), 73, 74
  - Online communications systems, 85
  - Operational wellness sessions, 88
  - OSI model, 24, 25
  - Overtaker rider, 252–253
  - Oxygen saturation monitoring, 56
- P**
- Parameter initialization, 250–251
  - Parasite power, 114
  - Particle swarm optimization (PSO), 150
  - Patients' health monitoring, enhanced
    - IoT-based array of sensors
      - abstract, 112–113
      - Bluetooth technology, 106
      - circuit design proposed, 116–117
      - comparison table, 121–122
      - dallas temperature sensor DS18B20, 114–115
      - data explosion and high expectations, 106
      - end-user healthcare applications, 107
      - ESP8266-1 Wi-Fi module, 115
      - health vitals, 120
      - heartbeat sensor, 111, 114
      - IoT patient health monitoring system, related studies on, 108–111
      - liquid crystal display, 115
      - microcontroller unit, 116
      - outputs, 119
      - proposed system, 114, 122
      - pulse sensor, 111
      - research and business, 108
      - ThingSpeak cloud, patient data stored on, 121
      - ThingSpeak web application, 119
      - ultraviolet detection sensor, 115
      - web application, 117–119
      - Zigbee module, 106
  - PEERP, 14
  - Performance metrics, 211
  - Permanent virtual circuit (PVC), 44
  - Pervasive monitoring system, 14
  - Physics-based algorithms, 245
  - Platform-as-a-Service (PaaS), 287, 288
  - Portable patchwork, 97
  - Post-COVID-19
    - digital technologies and innovations, 220
    - digitization and sustainability, 220

- Post-COVID-19 (*cont.*)
    - economic and environmental needs, 225
    - e-learning, 220
    - healthcare, 227
    - manufacturers, 227–228
    - smart farming, 226
    - transportation, 227
  - Precision-recall analysis, 215, 217
  - Predefined fitness function, 150
  - PriModChain, 356
  - Principal component analysis (PCA), 274
  - Privacy-enhancing technologies
    - access control, 322–323
    - cybersecurity, 319
    - encryption and communication protocols, 321–322
    - placing of, 320
    - protection and prevention approaches, 319–320
    - risk assessment, 323
    - secure boot, 322
    - security and privacy assessment, 323
  - Privacy issues, healthcare
    - confidentiality, 313
    - cybersecurity, 311
    - data eavesdropping, 313
    - identity threats, 313–314
    - inappropriate usage of data, 314–315
    - privacy-enhancing technologies
      - access control, 322–323
      - cybersecurity, 319
      - encryption and communication protocols, 321–322
      - placing of, 320
      - protection and prevention approaches, 319–320
      - risk assessment, 323
      - secure boot, 322
      - security and privacy assessment, 323
    - radio communication, 312
    - responsible parties
      - breaches, 315
      - ENISA's baseline recommendation, 318–319
      - liability of, 316–317
      - NIST's publication, 317–318
      - nonconfidential, 315
      - ransomware attack, 316
      - SciForce, 316
      - security policies, 319
    - unauthorized access, 314
    - user-pretending attack, 311
    - vulnerability exposure, 312
  - Wi-Fi networks, 312
    - WSN, 312
  - Privacy key management (PKM), 47
  - Private blockchain, 139
  - Procter & Gamble (P&G), 267
  - Proof of work (POW), 134
  - Protected health information (PHI), 131
  - Protocol for carrying authentication for network access (PANA), 40
  - Pseudonymity, 136
  - Psychotherapy, 161
  - Pulse sensor, 111
- Q**
- Q-learning algorithm, 275
  - Quick response (QR) cipher, 97
- R**
- Rackspace, 287
  - Radars, 85, 93, 95–97, 137, 140
  - Radial basis function (RBF), 166
  - Radio-frequency identification (RFID), 91
  - Random forest (RF), 273–274
  - Raspberry Pi, 12, 14, 15, 108, 109, 112, 113, 117, 181, 331, 363
  - Real-time IoT-based continuous glucose monitoring system, 195–196
  - Reduced carbon footprint, 292
  - Reduced e-waste, 293
  - Reference energy disaggregation dataset (REDD), 282
  - Rehabilitation systems, 57, 163
  - Reinforcement learning, 152, 275–276
  - Remote patient monitoring, 130
  - Repetitive high-amplitude activities, 160
  - Resource control management, 32
  - Resource optimization methods, 6
  - Respiratory illness symptoms, 88
  - RFID readers, 87–88
  - River formation dynamics (RFD) algorithm, 150–151
  - ROC curves, 214, 217
  - Routing protocols, 23
    - channel-aware routing protocol, 52
    - CORPL, 49, 52
    - MRPL, 49
    - P2P-RPL, 49
    - RPL, 49
    - scientific categorization, 50–51
- S**
- Secured smart healthcare monitoring systems
    - big data analytics, 128

- blockchain technology, 128–129
    - application of, 133–135
    - challenges of, 135–137
    - framework for, 137–140
  - computer and biomedical technologies,
    - integration of, 140
  - decentralized database, 128
  - Internet of Thing-based challenges in,
    - 130–132
  - Secure transactions, 293
  - Security issues, IIOT
    - AWSACIoT, 359
    - blockchain, 358–360
    - Dempster-Shafer theory (DST), 357
    - differential privacy (DP) policy model, 359
    - distributive nature, 358
    - identity-based signature (IBS), 359
    - Social Internet of Things (SIoT), 357, 358
  - Security protocol, 24
  - Self-isolation, 232
  - Self-organized agents, 150
  - Self-protection, 59, 88
  - Semantic medical access (SMA), 55
  - Semantic message-oriented middleware (SeMoM), 366
  - Sensors, 2
  - Sensory technologies, 174
  - Severe acute respiratory syndrome (SARS), 83
  - Sex attributes, 210
  - Shanghai Public Health Clinical Center, 94
  - Singular value decomposition (SVD), 274
  - 6LoBAC, 43
  - 6Lo-IPv6 (6Lo) working group, 40
  - 6LoWPAN, 37
  - 6 LoWPAN border routers (6 LBR), 42
  - Skin conductance (SC), 69
  - Smart city, 96, 97
  - Smart farming, 226
  - Smart fridges, 92
  - Smart gadgets, 9, 84, 85
  - Smart home ventilators, 93
  - Smart house appliances, 95
  - Smartphones, 57
  - Smart shelves, 92
  - Smart watches, 92–93
  - Social distancing, 92, 219, 228
  - Social Internet of Things (SIoT), 357, 358
  - Social media networks (SMNs), 166
  - Software-as-a-Service (SaaS), 287, 288
  - Spatio-temporal mathematical model, 223
  - Spontaneous facial reactions (SFRs), 68
  - Standardization, 139
  - Strain gauge sensor chest, 97
  - Strategic planning, 6
  - Subsystem optimization, 6
  - Supervised learning, 151
  - Support-vector machine (SVM), 69, 157, 160, 273
  - Support vector regression technique (SVRT), 279
  - Sustainable development goals (SDGs), 219–220
  - Swarm intelligence-based algorithms, 246–247
  - Synapses, 148
- T**
- Telemedicine, 30, 90
  - ThingSpeak, 117, 118
  - 3D printer, 93
  - Time-slotted channel hopping (TSCH), 38
  - TinyOS, 28
  - 6TiSCH, 38–39
  - Touch monitoring and detection software, 94
  - Traditional cloud computing, 290
  - Traditional neurocomputing methods, 68
  - Transportation security protocols, 24
  - Triple Data Encryption Standard (3-DES), 46
  - Troubleshooting, 24
  - 2014 TRUSTe IoTs Secrecy Survey, 94
  - T-shirt, 194, 195
  - T-test statistic, 72
  - Tuan Nguyen Gia's group, 70
  - Turing test, 151
  - Type 1 diabetes, 199
  - Type 2 diabetes, 199
- U**
- Ubiquitous communication, 87
  - UHF stickers, 87
  - Ultraviolet (UV) detection sensor, 115
  - UltraVo Energy (UEL), 44
  - Underwater wireless sensor networks (UWSN), 52
  - Unsupervised learning, 151–152, 274
  - Urbanization, 267
  - US Department of Defense (DoD), 22
  - User datagram protocol (UDP), 30
  - User interface (UI), 93
  - User-pretending attack, 311
- V**
- Vehicle-to-infrastructure (V2I)
    - communications, 31, 32
  - Vehicle-to-vehicle (V2V) mode, 277
  - Ventilators, 93

Verizon Cloud, 287  
VMware, 287  
Voice apps, 93  
VRTUS, 33

**W**

Warning system, 202  
Wearable biosensors, 202  
Wearable device access (WDA), 54  
Wearable patient care, 85  
Wearable Sensor Network (WSN), 137  
Wearable sensors, 92, 174  
Wearable technology, 165  
Web application, 117–119  
Web filtering techniques, 155–156  
WebSocket, 23  
Wheelchair management, 57  
Wide area networks (WAN), 22  
WiMAX, 46–47  
Wireless body area network (WBAN), 30, 86,  
129, 130  
Wireless body sensor networks (WBSNs), 278  
Wireless fidelity (Wi-Fi), 21, 86  
Wireless local area network (WLAN), 91

Wireless medical sensor network (WMSN),  
189

Wireless sensor network (WSN), 86, 189

Wireless sensor technology, 189–192  
Bluetooth, 190  
legal challenges, 193–194  
low energy requirement, 191  
patient data, 191  
security challenges, 192–193  
technology challenges, 194  
technology, reach of, 194–196  
ZigBee, 189

**X**

XMPP, 23

**Z**

ZigBee, 189, 195  
IP, 39–40  
module, 106, 109  
router, 39  
ZigBee End Device (ZED), 39