Advances in Science, Technology & Innovation
IEREK Interdisciplinary Series for Sustainable Development

Krishna Kant Singh · Anand Nayyar · Sudeep Tanwar ·
Mohamed Abouhawwash *Editors*

Emergence of Cyber Physical System and IoT in Smart Automation and Robotics

Computer Engineering in Automation

IEREK
RESEARCH & KNOWLEDGE ENRICHMENT

Springer

Advances in Science, Technology & Innovation

IEREK Interdisciplinary Series for Sustainable Development

Editorial Board

Anna Laura Pisello, Department of Engineering, University of Perugia, Italy

Dean Hawkes, University of Cambridge, Cambridge, UK

Hocine Bougdah, University for the Creative Arts, Farnham, UK

Federica Rosso, Sapienza University of Rome, Rome, Italy

Hassan Abdalla, University of East London, London, UK

Sofia-Natalia Boemi, Aristotle University of Thessaloniki, Greece

Nabil Mohareb, Faculty of Architecture - Design and Built Environment, Beirut Arab University, Beirut, Lebanon

Saleh Mesbah Elkaffas, Arab Academy for Science, Technology, Egypt

Emmanuel Bozonnet, University of la Rochelle, La Rochelle, France

Gloria Pignatta, University of Perugia, Italy

Yasser Mahgoub, Qatar University, Qatar

Luciano De Bonis, University of Molise, Italy

Stella Kostopoulou, Regional and Tourism Development, University of Thessaloniki, Thessaloniki, Greece

Biswajeet Pradhan, Faculty of Engineering and IT, University of Technology Sydney, Sydney, Australia

Md. Abdul Mannan, Universiti Malaysia Sarawak, Malaysia

Chaham Alalouch, Sultan Qaboos University, Muscat, Oman

Iman O. Gawad, Helwan University, Egypt

Anand Nayyar, Graduate School, Duy Tan University, Da Nang, Vietnam

Series Editor

Mourad Amer, International Experts for Research Enrichment and Knowledge Exchange (IEREK), Cairo, Egypt

Advances in Science, Technology & Innovation (ASTI) is a series of peer-reviewed books based on important emerging research that redefines the current disciplinary boundaries in science, technology and innovation (STI) in order to develop integrated concepts for sustainable development. It not only discusses the progress made towards securing more resources, allocating smarter solutions, and rebalancing the relationship between nature and people, but also provides in-depth insights from comprehensive research that addresses the **17 sustainable development goals (SDGs)** as set out by the UN for 2030.

The series draws on the best research papers from various IEREK and other international conferences to promote the creation and development of viable solutions for a **sustainable future and a positive societal** transformation with the help of integrated and innovative science-based approaches. Including interdisciplinary contributions, it presents innovative approaches and highlights how they can best support both economic and sustainable development, through better use of data, more effective institutions, and global, local and individual action, for the welfare of all societies.

The series particularly features conceptual and empirical contributions from various interrelated fields of science, technology and innovation, with an emphasis on digital transformation, that focus on providing practical solutions to **ensure food, water and energy security to achieve the SDGs.** It also presents new case studies offering concrete examples of how to resolve sustainable urbanization and environmental issues in different regions of the world.

The series is intended for professionals in research and teaching, consultancies and industry, and government and international organizations. Published in collaboration with IEREK, the Springer ASTI series will acquaint readers with essential new studies in STI for sustainable development.

ASTI series has now been accepted for Scopus (September 2020). All content published in this series will start appearing on the Scopus site in early 2021.

More information about this series at http://www.springer.com/series/15883

Krishna Kant Singh · Anand Nayyar ·
Sudeep Tanwar · Mohamed Abouhawwash
Editors

Emergence of Cyber Physical System and IoT in Smart Automation and Robotics

Computer Engineering in Automation

Springer

Editors
Krishna Kant Singh
Department of Computer Science & Engineering
Faculty of Engineering & Technology
Jain (Deemed-to-be University)
Bengaluru, India

Anand Nayyar
Graduate School, Faculty of Information Technology
Duy Tan University
Da Nang, Viet Nam

Sudeep Tanwar
Department of Computer Science and Engineering
Nirma University
Ahmedabad, India

Mohamed Abouhawwash
Department of Computational Mathematics, Science, and Engineering
Michigan State University
East Lansing, MI, USA

ISSN 2522-8714 ISSN 2522-8722 (electronic)
Advances in Science, Technology & Innovation
IEREK Interdisciplinary Series for Sustainable Development
ISBN 978-3-030-66221-9 ISBN 978-3-030-66222-6 (eBook)
https://doi.org/10.1007/978-3-030-66222-6

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021
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

Preface

According to National Science Foundation (NSF), cyber-physical system is defined as "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components"—that is cyber and physical components. In the past few years, science and technology has undergone tremendous change in terms of computing, communications and control to support and advance varied domains, and this has led to connectivity of almost everything to the cyberspace. Cyber-physical systems main idea is to use computing (sensing, analysing, predicting, understanding), communication (interaction, intervene, interface management) and control (evolve and interoperate) to make intelligent and autonomous systems. The vision of IoT assumes that networked connection of smart things, i.e. cyber-physical systems, with sensors and actuators that influence the physical environments has strong potential to add novel services to the society. Communication is vital in cyber-physical system, as they allow different objects to exchange information with each other and with humans, at any time and in any conditions.

The underlying idea for offering this book titled *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation* is to understand the current and future impact of cyber-physical systems, IoT and IIoT cum IIoT in the future world and to study its potential socioeconomic impacts. We believe that this book will bring a strong knowledge base for readers in cohesive manner to understand CPS and visualize its growth, issues and connected applications in coming few years.

This book consists of 14 chapters, contributed by leading authors in the field, covering diverse aspects of cyber-physical systems, Internet of Things, Industrial Internet of Things, robotics, security issues and connected technologies. Chapter titled "IoT-Aided Robotics Development and Applications with AI" highlights scientific consequences, open problems, challenges and target applications in Internet of Robotic Things (IoRT). Chapter titled "Convergence of IoT and CPS in Robotics" focuses on how two different aspects IoT and CPS converge together in robotics industry making it more efficient and pleasing to adapt by other organizations, institutions, etc. Chapter titled "IoT, IIoT, and Cyber-Physical Systems Integration" focuses on the integration of IoT, Industrial IoT and cyber-physical systems and covers analytical data on industrial revolution and Industry 4.0 and covers several aspects regarding history, development trends, definitions, architectures, components, applications and characteristics. Chapter titled "Event and Activity Recognition in Video Surveillance for Cyber-Physical Systems" proposes the development of cyber-physical system in automated understanding of events and activity in various applications of video surveillance by exploiting temporal features using a hybrid convolutional neural network + recurrent neural network architecture and recorded on four benchmark datasets, i.e. Columbia Consumer Video (CCV), Human Motion Database (HMDB), UCF-101 and Kodak's Consumer Video (KCV). Chapter titled "An IoT-Based Autonomous Robot System for Maize Precision Agriculture Operations in Sub-Saharan Africa" proposes a novel design of IoT-based autonomous robotic system for precision agricultural operations in maize crop production for improving crop yield, profit and improved revenue from agriculture. Chapter titled "A Concept of Internet of Robotic Things for Smart Automation" provides an overview of possible solutions for various issues in smart automation environment and applications of robotics using Internet of Things and visualize the impact of IoRT in the future connected world. Chapter titled "IoT in Smart Automation and Robotics with Streaming Analytical Challenges" highlights the importance of fusion of robotics, IoT and artificial intelligence to perform complex assignments, automation and mankind help, and the chapter discusses various case studied and applications regarding IoRT. Chapter titled "Managing IoT and Cloud-Based Healthcare Record System Using Unique Identification Number to Promote Integrated Healthcare Delivery System: A Perspective from India" highlights the importance of IoT and cloud-based medical record system and proposes a novel model to use UID, IoT and cloud computing for healthcare orientations. Chapter titled "Internet of Robotic Things: Its Domain, Methodologies, and Applications" highlights the concept of IoRT and its connected technologies and applications and also proposes a smart IoRT-based architecture for smart library management. Chapter titled "Applications of GPUs for Signal Processing Algorithms: A Case Study on Design Choices for Cyber-Physical Systems" highlights the hardware implementations of different signal processing algorithms by showcasing appropriate hardware platforms and various open-source languages. Chapter titled "The Role of IoT and Narrow Band (NB)-IoT for Several Use Cases" presents the role of IoT and NB-IoT for several use cases, such as intelligent healthcare for people, smart agriculture devices of NB-IoT, livestock tracker, greenhouse sensors, pollution detection in NB-IoT, fog computing in NB-IoT for air pollution detection, intelligent garbage bin in smart cities, smart parking, fog computing approach for smart parking, smart factory, OneNet platform and NB-IoT for maritime use case. Chapter titled "Robust and Secure Routing Protocols for MANET-Based Internet of Things Systems—A Survey" discusses various existing secure MANET protocols that provide secure data transmission and can also be used in the IoT environment to provide robustness in the presence of a variety of threats and vulnerabilities and also presents some major challenges in the emerging domain of MANET-based IoT systems for robotics. Chapter titled "IoT for Smart Automation and Robot " discusses the importance of intelligent IoT devices and robotics today and in the future in the domains like home automation, industrial automation and city automation. Chapter titled "Application of Internet of Thing and Cyber Physical System in Industry 4.0 Smart Manufacturing" discusses the effects of IoT technology and CPS in the advancement and awareness of real-life smart manufacturing, and an integrated IoT and CPS framework is recommended as a specification for researchers and industries towards the full realization of the potentials of IoT with CPS in the development of industry 4.0 smart manufacturing technologies.

Bengaluru, India	Krishna Kant Singh
Da Nang, Viet Nam	Anand Nayyar
Ahmedabad, India	Sudeep Tanwar
East Lansing, USA	Mohamed Abouhawwash

Contents

IoT-Aided Robotics Development and Applications with AI

Amrita Rai, Deepti Sharma, Shubhyansh Rai, Amandeep Singh,
and Krishna Kant Singh

Abstract

Global research and developments in robotics and IoT have received noteworthy consideration in the present years. The chapter highlights some efforts of researchers in robotics and artificial intelligence using IoT applications and advancements. The intelligent robotics structures exploit the physical shapes of robotics and have the ability to think and perform duties like human beings. Artificial intelligence focusses on the aspects like how the robot or machine performs duties, such as reasoning, learning, and problem solving. The IoT of robotics is an emerging area of research and development that brings together universal sensors and autonomous systems. The fusion of robotics and IoT technologies will increase the capabilities of new creation in both the existing IoT and the robotics systems. Integration of the IoT and robotics gives birth to new concept titled "Internet of Robotic Things (IoRT)"; it talks about the beginning of cloud robotics and its support toward robotic functions like sensing, manipulation, and mobility. The IoRT-aided systems are very useful in various applications of every domain in life like medical, defense, farming, industrial plants, and rescue operations. Moreover, the track to an established evolution of IoT-aided robotics products needs several essential issues to be resolved, designing methods to be associated, and strong structural choices to be deliberated. This chapter covers scientific consequences, open problems, challenges, and target applications in the IoRT area. In today's scenario, IoT-aided robotics has diverse fields and services like: communication networks, distributed and pervasive computing, semantic-oriented approaches to consensus, network security, and many others.

Keywords

IoRT (internet of robotics things) • Cloud robotics • Artificial intelligence • Edge computing

1 Introduction

Everything we see in today's world is a boon of the Internet. The Internet has provided us with numerous advantages that lead the world toward automation and the interconnection of machines with the Internet to reduce man-to-man and machine-to-man interactions, which is referred to as Internet of Things (IoT). IoT plays a vital role in making a machine smart enough to perform various things on its own and hence reduces the man labor to perform the same task with the same precision (Roy Chowdhury, 2017). The concept of IoT has always fascinated numerous people to use, study, and research more about it and explore the concepts in depth as highlighted in Fig. 1. We might have seen in various sci-fi movies about glimpses of the future world and how it looks like, and with IoT, we get an opportunity to experience the trends in technology. There are several applications in the

A. Rai (✉)
Department of ECE, G. L. Bajaj Institute of Technology and Management, Greater Noida, India
e-mail: amritaskrai@gmail.com

D. Sharma
Department of CS, KCC Institute of Technology & Management, Greater Noida, India
e-mail: Deeptiguria@gmail.com

S. Rai
Department of Artificial Intelligence, Gautama Buddha University, Greater Noida, India
e-mail: shubhayansh@gmail.com

A. Singh
Department of ECE, KCC Institute of Technology & Management, Greater Noida, India
e-mail: suriaman119@gmail.com

K. K. Singh
Department of Computer Science & Engineering,Faculty of Engineering & Technology, Jain (Deemed-to-be University), Bengaluru, India
e-mail: krishnaiitr2011@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_1

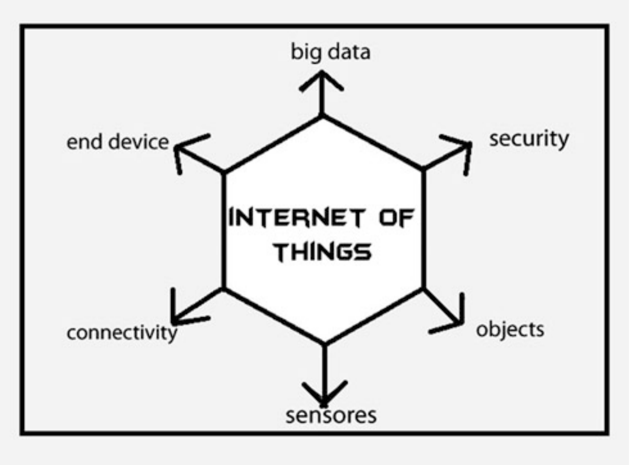


Fig. 1 Entities of IoT

market now which uses the concepts of IoT to make our lives easier by interconnecting it with different sensors to obsolete manpower. IoT has made cities smarter through its applications which is attracting more people toward them and hence helping in the growth of the nation (Vermesan et al., 2017). From home to offices and from hospitals to military ground, it has proved to be useful in various dynamic situations (Ray, 2016).

IoT has proved to be a revolutionary technology where smart things communicate with each other with the help of the Internet, to bring out some useful actions to make our lives easier. The main motive behind this technology is to help people with basic programming experience to construct some smart ideas into reality on their own. One can create a lot of things by compiling small fragments of codes into an effective program. On the other hand, robotics is another futuristic technology that includes designing, assembling, functioning, and usage of robots. Robots are accessible to reach each and every corner where humans cannot, such as the rover which touched the surface of Mars was a robot (Kehoe et al., 2015). Even, robots are serving people in place of humans in the pandemic. They are well trained to behave similarly to humans and can respond according to the situation. They made our life easier by plunging the workload of mankind, and with the study, it is found that robots are more précised than humans. Robots are sophisticated, intelligent systems used in various applications such as an assistant to a pilot, wherever more skill is required, and in several space operations (Rai et al., 2021).

With the recent development of robotics and automation in industrial applications, it led to think more about the controllability of the machines remotely and in the same instance remotely monitor environmental parameters via the help of sensors such as temperature and pressure (Grieco et al., 2014). To bring this into existence, IoT and robotics are clubbed together so that they can collectively work better for the welfare of the society. Robotics allows the user to design, optimize, and function according to the need, whereas the IoT helps the robot to establish connections with another smart machine. Robots either can be operated manually or can be controlled by some predefined functions which are often referred to as programs.

Various sensors (proximity sensor, IR sensor, and more) are used to perform different functions (obstacle detection, line-following, and more) as per the need of the user. These sensors are either assembled on a breadboard or to the PCB (printed circuit board), whereas for IoT, Raspberry Pi is considered to be one of the most prominent platforms to perform various things (https:www.therobotreport.com/10-biggest-challenges-in-robotics). Because of its compact size, low cost, and versatile nature, it is widely used in most of the applications for IoT. IoT-aided robotics has emerged with several applications which mankind has never imagined before. The remote controlling feature gives it more feasibility to access anything from anywhere, anytime.

In upcoming years, the technological trends are expected to go beyond imagination. Each and everything which we have never imagined will be in reality. The emerging skills will help people to learn and implement more smart things that will contribute to enhancing our lifestyle and life expectancy rate. In this chapter, we review the recent work in the area of cloud computing needs in the field of IoT and robotics and various issues of integration of IoT with cloud computing technology. We draw insights about the recent role of robots as hub and gateway devices and mainly discuss the utilization of IoT-aided robots in a different domain, challenges, and limitations in the implementation of such robots, research perspective of above, and future scope for further research.

Organization of Chapter

This chapter is organized as follows: Sect. 2 highlights the role of cloud computing in IoT and robotics. Section 3 explains the robots as edge devices and gateways. Section 4 describes the applications of IoT-aided robots in industries and all over the real world. Next, Sect. 5 discusses the challenges in AI-based robotics development. Finally, Sect. 6 presents our conclusion and future scope.

2 Role of Cloud Computing (Cc) in IoT and Robotics

The IoT-aided robotics companies have so far been running over different substituent objectives. The key focus is on supporting information on pervasive sensing, tracking, and monitoring—further on the manufacturing action, autonomous behavior, and interaction between machine to machine and man to machine. For this reason, it is highly claimed that the interference of IoT and robotics will bring a strong added trait in the technology and set a remark in the technology. Early signs of IoT-aided robotics unification can be observed in distributed, heterogeneous robot control models like network robot systems or robot ecologies and cloud robotics that impart source-intensive features on the server-side. The term "Internet of Robotic Things" is introduced to the concept where sensor data from numerous devices is taken, processed, and distributed intelligence and is used to control the entities in the physical world. In the cyber-physical perspective of the Internet of Robotic Things, sensors, and data analytics of the IoT will be used to provide robots a broad situational awareness that leads toward the better functioning of the robots. Further, Internet of Robotics achieves alternate visions of this term (Vermesan et al., 2017; Ray, 2016; Kehoe et al., 2015; Rai et al., 2021; Grieco et al., 2014; Talwana & Hua, 2016; Silva et al., 2019; Islam et al., 2012; https:www.therobotreport.com/10-biggest-challenges-in-robotics).

As we know IoT has allowed us to perform several tasks just by sitting in the comfort of our home when merged with robotics, it leads towards the present smart world (Talwana & Hua, 2016). However, there is still something missing that is not leading us to achieve the best of the latest technology and services, which is the conflict with the data. Earlier data can be stored in memory with the help of devices such as compact disk (CD), DVDs, floppy disk, hard disk, and pen drives; however, due to their compact size, limited storage capacity, and local usage, it becomes difficult to access data anywhere, anytime.

Cloud computing (CC) is one of the biggest technological revolutions around us. It is changing how the consumers consume services, and how the organizations manufacture and function applications and completely reshaping the old business models in multiple industries. It is providing a growing amount of opportunities for a small and big business to expand into new markets, innovate more quickly, and create new value. Applications and data stored in the cloud can be managed and operated by someone else and the end-users are using cloud-based services from any location globally. Cloud computing is touching almost every corner of our life (Silva et al., 2019). It is transforming the IT world, and the impact wave is growing and spreading around.

Cloud computing is user-centric, task-centric, and secure technology which provides services such as storage, network, database, identity, and platform and helps in communicating with different machines and networks. Cloud computing proves to be the best platform for every group of the user whether it be a small businessman or a big firm everyone takes the benefit of the services of the cloud by paying some certain amount as per the services chosen by the customer (Islam et al., 2012).

Cloud computing offers a reliable platform which is the major requirement of the IoT platform. The cloud is not only used to share the resources but also helps in increasing the resource capacity. With the help of an Internet connection, anything can be accessed globally without any problem similar to IoT; everything should be accessed through any location worldwide. The virtualization of physical devices is another vital trait of cloud computing and makes it homogenous. It allows resource sharing features to several users. Cloud provides elasticity and scalability of resources and applications which further leads to high availability and accessibility of the resources; hence, the collaboration of IoT and cloud computing can bring enormous opportunities in both fields (Biswas et al., 2014).

Many researchers are working on the idea of making robots through the help of the cloud, which is known as cloud-based robotics as shown in Fig. 2. A professor from Carnegie Melon University stated the possibility of assembling cloud services with robotics to maximize its efficiency and to diversify working functions. Bulky CPU tasks can be discharged to small and low power mode remote clouds. The ability of a robot can be enhanced by fusing it with the services of the cloud. A live illustration of this is Google's cloud-enabled goggles which can tell about the object which we have never seen before through the algorithms designed and saving that new data to the cloud (https://www.uipath.com/blog/solving-robotic-ai-challenges). Apart from all the advantages we have studied so far, J P Laumond highlights some disadvantages of cloud-aided robotics in (Guizzo, 2011). According to J. P. Laumond, the cloud would not be able to help in achieving appropriate real-time performance relying upon the strong on-board assembly of sensors. For instance, the motion-controlled robots can easily work by communicating with the assembled sensors rather than with the cloud (Du et al., 2016).

The principal objective of the robot cloud is to make robots a part of CC service which leads to the concept of "Robot as a service." The robot service architecture is not

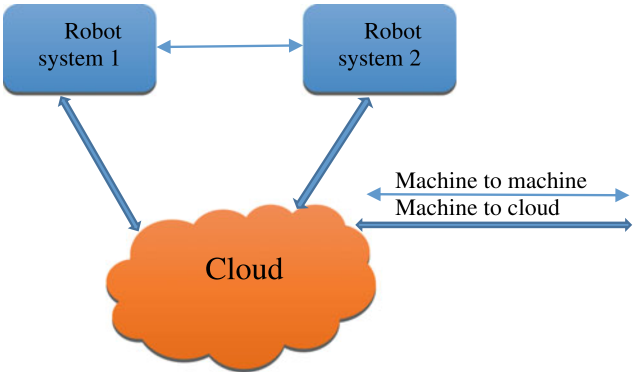


Fig. 2 Cloud-aided robotics

built on the web and hence results in simpler and faster interfaces. Services are also flexible to run on a local device to deduct the cost of communication. Robots in the robot cloud can communicate with each other so that the data can be shared among them and finish the need to send data manually to different machines. As a result, the robot cloud will utilize the best features of the two technology and will be able to contribute more effectively to the growth of the industry.

2.1 IoT and Cloud Computing (Cc)

The objective of cloud computing is to allow customers to access data from anywhere, anytime therefore limiting the requirement of hardware equipment. The term cloud computing is defined as the prepaid services provided to the customer according to the user through the Internet. The services may include databases, servers, networks, applications, and platforms. These days, cloud computing has taken over the market with all the above-mentioned features for the growth of the industry and allows the employees to do work from the comfort of their home (https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade). CC is the technology that can be set as a base technology in the utilization of IoT as shown in Fig. 3.

The integration of cloud computing with mobiles to make cellular phones more resourceful in terms of computational power, database, content management, and energy is known as mobile cloud computing. Cloud computing can relate with some salient features of IoT such as:

a. Database over Internet
b. Services over Internet
c. Applications over Internet
d. Computational capability
e. Energy efficient.

We have an opportunity to maximize the use of available technology that is incorporated with the cloud environment by integrating cloud computing and IoT. Applications and services that use IoT technology can be accessed when combined with cloud storage. The merging of CC with IoT is shown in Fig. 1. Cloud provides a platform for mobile and wireless users to use all the necessary information and applications for IoT connectivity (Stergiou et al., 2016). Table 1 describes the comparison between IoT and cloud computation. One of the most popular IoT with a cloud integration platform is Amazon Web Services (AWS), and others are ARM GE Predix, Google Cloud IoT, and Microsoft Azure.

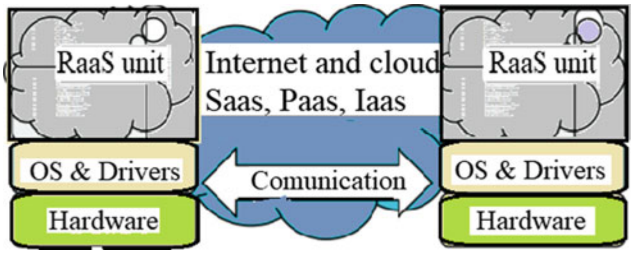


Fig. 3 RaaS in cloud computing and IoT

2.1.1 Application and Security Issues of Cloud Computing and IoT Integration

We have observed a rapid and independent evolution in both the word IoT and cloud computing. Through the combination of IoT and cloud computing, cloud computing can cover up the limitations of IoT such as limited storage and applications over the Internet. Similarly, IoT hinders the limited scope of the cloud. The security issue of this integration has always been a matter of chaos. Trust issues, limited knowledge about the service level agreements (SLAs), and knowledge about the physical location of data arise concerns about merging IoT and cloud computing technology. Data security is a topic of discussion in IoT as well as cloud Computing. Multi-tenancy could be another subject that leads to compromise security and sensitive information can be leaked. Moreover, due to computing power constrain in things, we cannot apply cryptography to all the layers (Aazam et al., 2014).

Application and challenges about the security issue in the unification of two diverse technologies are shown in Fig. 4 and explained below:

Heterogeneity: One of the biggest problems in IoT and cloud computing is the diversity of devices, operating systems (OS), platforms, applications, and new services provided from time to time.

Performance and Big Data: With the growth of data and unpredictability also comes into play the quality of service (QoS) which becomes a subject of concern. In any instance, any type and quantity of data can be set off. On the cloud side, we require dynamic prioritization of the requests. QoS is usually measured in terms of bandwidth, jitter, packet loss ratio, and delay, depending upon the urgency and type of data to be sent on the sync node (Stergiou et al., 2018).

Monitoring and Reliability: Monitoring is one of the important activities in the cloud for capacity planning, managing resources, SLAs, performance, and security. Cloud of things inherits monitoring skills from the cloud but affects volume, variety, and velocity challenges of IoT. The concern of reliability arises in the case of vehicular networking and communication. The reliability of the devices is enhanced using the cloud by allowing to offload heavy tasks which leads to increase devices' battery duration or proposing the possibility of developing a modular structure

Table 1 Comparison of IoT with cloud computing Integration

S. No.	Items	IoT	Cloud computing
1	Processing capability	Limited computational processing capability	Virtually unlimited computation processing capability
2	Characteristics	IoT is pervasive (things are everywhere). These are real-world objects	Cloud is ubiquitous (resources are available from everywhere). These are virtual resources
3	Connectivity	It uses the Internet as a point of convergence	It uses the Internet as service delivery
4	Storage capabilities	Limited storage or no storage capabilities	Unlimited storage capabilities
5	Big data	It is a source of big data	It is mean by which to manage big data

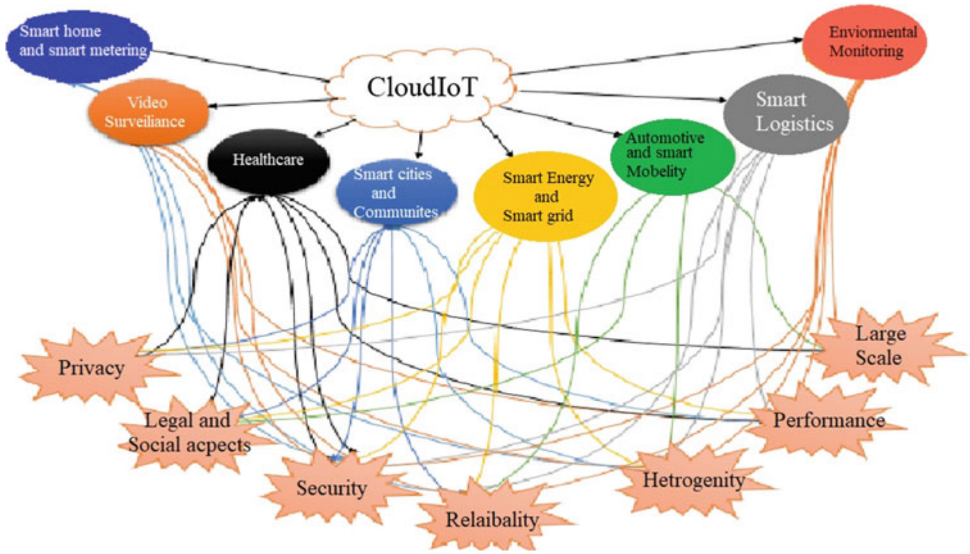


Fig. 4 Application and security issues of integrating IoT and cloud computation

(Yun & Yuxin, 2010; Wang et al., 2014; Rao et al., 2012; Kuo, 2011).

Wide-Ranging: Cloud of things allows us to design innovative applications giving more emphasis on unification and examination of data coming from real-time devices (Petrolo et al., 2014; Lazarescu, 2013; Bo & Wang, 2011; Mitton et al., 2012; Rao et al., 2012; Xiao et al., 2013). Sometimes devices need to interact with the large number of devices distributed in a wide area. The requirement of storage and computational for the other processes is a challenge that is hard to overcome.

Sensor networks and Fog computing: Sensor networks are the key to IoT (Zaslavsky et al., 2013) and one of the five important technologies contributing in the modern world allowing us to do measurements and acknowledge environmental indicators, from fragile sustainable resources and ecologies to urban ambiance (Gubbi et al., 2013). Recent trends in technology helped in large-scale production of miniaturized low-cost and low-power devices for remote sensing applications (Akyildiz et al., 2002). These miniaturized devices (mobile phones) come with a variety of sensors enabled in it (GPS, gyroscope, fingerprint sensor, etc.) enabling a broad range of IoT applications in different sectors. Moreover, when they communicate with each other and form networks, supporting the IoT applications is characterized by constraints and for mobility requirements and geo-distributions (Bonomi et al., 2012).

2.1.2 Protocol Support and IPv6 Deployment in IoT and Cloud Computing Integration

To connect with various devices for the integration of various sensors, we need the concept of IoT, and to provide control to the application, we need to use cloud computing to add more functionality, but there must be something which should monitor every communication link so that the application, server, or network should be used more effectively. So, a protocol suite is required to take care of application, server, or network. A protocol is nothing but a set of rule and regulation which needs to be obeyed by the computer and data every time. The protocol controls the communication; they monitor the flow of data across the end-users and restricts any unethical activity.

For the connectivity of different things, we have a variety of protocols. Even if there are similar systems, there is a probability that they may work on non-identical protocols such as sensor IoT in which sensors like Zigbee module, Wireless HART, IEEE 1451, etc. Some of them will be supported by the gateway devices but some may not. The only solution for such kind of problems is the mapping of protocols in gateways.

Internet Protocol (IP) has two different versions IPv4 and IPv6. Earlier, all the major work was done over the IPv4, but due to its small header size it becomes more problematic to perform some functions and the cybercrime cases were also rising so we need a secure IP version to maintain the balance. IPv6 was another proposed model that is being used presently and offers a 128-bit header size and most importantly it is secure (Wu et al., 2013). IPv6 uses all the protocols used by IPv4; in addition to it, some new secure protocols were introduced for the confidentiality of the data. IPv6 allows the identification of the devices connected to the Internet which helped in decaying the cases of cybercrime (Babatunde, 2014).

2.1.3 Resource Allocation and Location of Database in IoT and Cloud Integration

It would be a chaos if the IoT of two entirely different devices will request for the data on the cloud due to the difficulty in deciding about the volume of data required by the individual device. With the help of mapping, the resource allocation can be completed by identifying the type of sensor, volume, and rate of occurrence of data production. Sending a sample packet from a newly added node can also be productive.

Location plays an important role in fast processing (reception and transmission) of data. Time-sensitive data such as video and audio should be shared within small ranges for the fast and complete transmission. Irrelevant data can be sent at any stage once the device is connected to the Internet. To control the transmission of unnecessary data, we need to use smart gateways that keep an eye on the quality of the data (Aazam, 2014; Stergiou et al., 2018; Yun & Yuxin, 2010; Wang et al., 2014; Rao et al., 2012; Kuo, 2011; Petrolo et al., 2014; Lazarescu, 2013; Bo & Wang, 2011; Mitton et al., 2012; Xiao et al., 2013; Zaslavsky et al., 2013; Gubbi et al., 2013; Akyildiz et al., 2002; Bonomi et al., 2012; Wu et al., 2013; Babatunde, 2014).

2.2 Robot as a Service in Cloud Computing (RaaS)

Ideally, robots are perfect examples of smart hardware devices. A small robotics system conveys a sense that it has intent or agency of its own through its appearance and movements (Chen & Hualiang, 2013). There are three aspects which are required to be studied: structure, interface, and behavior.

The requirement and structure features of RaaS in cloud computing environments are multiple and can be used in various ways: robot cops (Bertelsen & Bødker, 2003), restaurant waiter robots (Tsai et al., 2005), robot pets (Nayyar et al., 2018) and care-taking robots (Sehgal et al., 2020) These robots can be distributed globally and their services can be utilized from anywhere and at any time with the help of the Internet. The fundamental requirement for RaaS is to have complete functionality over the functions of SOA, that is, as service provider, service broker, and a service client. The SOC software in RaaS would communicate with all the drivers which are being used and other operating systems. RaaS units can directly communicate with other RaaS units with the help of Wi-Fi or ad hoc wireless networks. The communication between RaaS and other units is standard.

Various research works had been done earlier as well on an initial basis which consists of the basic understanding of activity (Tsai et al., (2005),) action, and operation of RaaS. Process Specification and Modeling Language for Service (PSML-S) has been developed to describe the behaviors in a service-oriented computing model (Gupta et al., 2020). It describes the relationship between conditions, data, actors, actions, timing, and events. The studies are building foundation for a new standalone processing technology theory which is making decisions based on the context and situations.

An illustration in Fig. 3 describes different contexts we are dealing with and how the RaaS units behave under such an environment. A soccer game is defined in which we have three robots as players: a striker, second striker, and a goalkeeper when playing offense, while playing defense the possible roles which the bots may have to obey are center back, sweeper, and a goalkeeper.

Ruleset

Primary striker: The role is to carry the ball in the direction of the valid goal, must avoid the defenders, and pass the ball to the other teammate whenever it is required. Once the ball is passed to the secondary player, then it should act like the primary player and follows all the above rules.

Secondary striker: It moves to a position that is closer to the goal and far away from the defenders to prepare to receive the ball from the first player, and once it gets the ball, it transforms itself into primary player and the other one will act as secondary player.

Center back: It focusses on the defense side to defend the player with the ball to attack.

Sweeper defends the secondary striker and back up at the center. If the ball is passed from the primary player to the second player, then the center back and sweeper will swap the roles. Goalkeepers usually stay in the goal area to defend the attack. In some situations, the goalkeeper can leave the goal area and become a third player. The entity, actions, attributes, and the values can be defined as element. Entity refers to an element in the game and it is defined by (N, P, V), where N is name, P is attribute, and V is value of the attribute. Here, we have two kinds of entities: robots and a ball.

A robot has following properties: (*X*, *Y*, down, action, relation), where *X* and *Y* will define the coordinates of the robot down, is a Boolean variable which indicates the active state or ON state of the robot. Actions can take only five values as discussed earlier.

The ball has the following properties: (*X*, *Y*, direction, speed) *X* and *Y* describe the present position of the ball. Direction and speed define the direction of propagation.

The game includes the properties of the ball, robot, and derived properties like who is having the ball, number of robots in a particular area. Since we can expect spontaneous changes in the position of balls, so there might be multiple changes of actions of each bot. Now, the robots itself have to decide what they have to do and make their own decisions.

3 Robots as Edge Devices and Gateways

Except for being supportive in nature, the robot can also act as a hub or even as a gateway device. Robots are generally provided interfaces to the LAN or Wi-Fi networks, sometimes with Bluetooth (BT), XRF, and others. Smart robotics is driven by data analysis, advanced AI, and networking working together to create more reliable self-driven devices (Kaelbling, 1988; https://tdwi.org/articles/2020/04/27/arch-all-smart-devices-and-coming-of-edge-computing.aspx). Edge computing provides hold to devices or gateways on the network. The fundamentals are determined by the thought that it is necessary to do some processing with extremely fewer inputs provided to feed processes such as local analytics, robotic functions, and sensor actions. Strong devices and gateways help to compress data for transmission to the cloud, perform preprocessing, and perform automatic tasks without any need of a central computer. Thus, due to these competencies, the development of IoT and 5G networks will gain more attention. Hence, there is a high demand for supporting infrastructures and new security systems and models for processing data of IoT as primary task (Schlussel, 1983; Verma & Kumar, 2018; Lekkala & Mittal, 2015).

Figure 5 highlights the main components of robotics and IoT architecture. It shows both edge side and cloud side of computations. The basic components like sensors, actuators, hardware devices, and crucial things at the edge side are called gateway and have responsibility for establishing communications between devices and cloud services, and also coordinating the actions between things and devices (Verma & Kumar, 2018; Lekkala & Mittal, 2015; Leng & Mital, 1989; Lund, 2004; Bamdale et al., 2019).

3.1 Use Cases

Registering as close as conceivable to the point of utilization has consistently been significant for products requiring low-inertness information transmission, exceptionally high data transmission, or ground-breaking nearby handling capacities

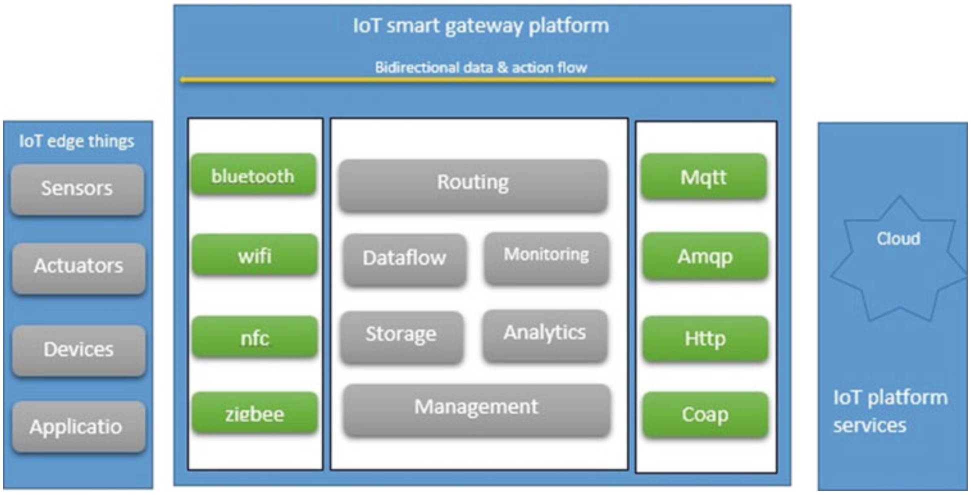


Fig. 5 Component of robotics and IoT architecture at the edge

—especially for AI (ML) and different investigation (Lund, 2004). Edge figuring is growing an arrangement of utilization cases that incorporate self-ruling gadgets, modern mechanical autonomy of Industry 4.0, brilliant residential gadgets, AR/VR, telco capacities, artificial intelligence and machine learning, medication, and funds. In every one of these zones, it is conceivable to discover situations where insignificant inertness and gigantic neighborhood preparation can be of a preferred position. Be that as it may, investigators see this going a lot further—and numerous companies concur (Leng & Mital, 1989).

3.2 Condition of the Edge

Since it is viewed as the latest innovation, numerous organizations have got on board with the edge registering fleeting trend. Advancement is moderate and the required advancements are not yet set up, yet limited open doors can be found in about each region. Edge figuring is dispersed, decentralized processing that puts critical force proximate to the end-client area. Thus, it is a characteristic advancement in expanding PC force and portability. The large change will come when framework ideas are normalized with accessible programming set up, 5G systems arrive at full activity and are accessible all-inclusive, guidelines are delivered for the Internet of Things segments, and costs start to descend so the IoT itself starts to develop (Bamdale et al., 2019).

3.3 The Bandwagon

This is energizing stuff and is a result of the development of 5G organizing, expanded extension of the Internet of Things, development of utilization cases, and expanded consideration (for instance, because of high deceivability of driverless vehicles) alongside a steadily developing comprehension of what the 5G system may achieve. Much isn't yet known; current executions will in general be profoundly exclusive and to some degree constrained. This implies that the duplication of fruitful cases is unmistakably progressively difficult. Nonetheless, edge figuring is unquestionably in transit and it is critical to get ready for this new future era. This is a test-driven vision that joins many developments in both artificial intelligence and systems administration to make all the more notable confined frameworks (Verma & Kumar, 2018; Lekkala & Mittal, 2015; Leng & Mital, 1989; Lund, 2004; Bamdale et al., 2019; Global Employment Institute Artificial Intelligence and Robotics and Their Impact on the Workplace, 2017; https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/a-robot-that-explains-its-actions).

3.4 Intelligent Agent

By the study of intelligent agents, AI and robotics come closer to others. These are machines having somatic relations with the world. Some key applications of intelligent agents include military missions (such as enhanced integration and sensors) and other diversified areas. AI community can reward huge work on the intelligent agents by putting the focus on various problems as it will improve the techniques. Moreover, it will be in charge of the AI community to form a system that can merge the information gathered by agents' sensors.

In the late 1960s, Shakey was one of the first intelligent robotic agents by SRI international to set out for improved software and hardware technologies. It worked in the artificial blocks world by recognizing its ambiance with a computer vision system and laser rangefinder. The work inspired many AI systems such as the STRIPS planning system and supported STRIPS to determine the number of actions that can help them in reaching the desired goal. It also helped in learning about macro-operators.

However, the Shakey project was an achievement and it worked on speeds that made it inappropriate for real applications.

3.5 Scope for Intelligent Agents

Approaches regarding modification of PC visions focus on the study of one image without having any prior information. Some techniques are of substantial theoretical choices and have applications in the examination of still images.

By looking at the importance of that thing, vision can be done more effectively. It is the essence of the model-based vision. Another way of getting information is by building low-level visual processes into agents like virtual sensors. For example, a bot that directs the hallways in the office ambiance can get a great deal of information simply by knowing the position of the rows. Vision can also be helpful in many other ways. Stereo cameras can help to recognize a particular thing. Algorithms of stereo vision are costly, but they can be made more effective by using a low-resolution image instead of high-resolution images.

3.6 Planning and Action

Shakey is mainly used in the model of planning which mainly required a sequence of effective actions, and it has been extensively studied in the AI community. Now and again, we have to stop and deal with the most effective client sequence in which we can perform a set of errands or a route on a map, but that type of activity is very much conventional. For this logic, more or less of artificial intelligence and cognitive science analyst study planning. This study shows a unique mankind activity that depends upon experienced intelligence system. Many of those whose aim is to develop intelligent agents have chosen to focus in its place on developing a mechanism for regular performance rather than planning.

In an influential world, two practical grounds that influence them are:

1. The current state may change in accordance to make the plan invalidate during the time.
2. The agent may ignore the sensory inputs from the system which may cause it to be endangered.

With the help of reactive planning, it maintains a strategic distance from these types of above barriers in which the agent embarks on the performed plan but continuously monitors the world to assure itself that the plan it is executing is indeed appropriate to the circumstances. Another methodology is to plan the specialist to go about however much as could be expected dependent on sensory inputs of info, which can avoid the computational and semantic troubles of large information base of realities. Even if this model effort the maximum reactivity, but still it is vulnerable to the several critics of incentive response systems.

Which the operator leaves on the performed arrangement however ceaselessly screens the world to guarantee itself that the arrangement is executing undoubtedly proper to the given conditions. Another methodology is to plan the specialist to go about however much as could be expected dependent on tactile sources of info, dodging the computational and semantic troubles of an enormous information base of realities.

3.7 Applications of IoT-Aided Robot

The collaboration of the Internet of Things and mechanical autonomy remains to a great extent an undiscovered field of future innovation that can realize radical changes to how we live these days. IoT-based arrangements are changing how we tackle issues. Savvy homes, wearable, brilliant urban areas, keen networks, mechanical web, associated vehicles, associated well-being, shrewd retail, shrewd flexibly chains, and brilliant cultivating are just a couple of the IoT apps in today's times which have affected how we live as the general public. By giving ongoing, quantifiable, and conclusive information, the Internet of Things has diminished our reaction time to basic issues and in a couple of cases made expelled the requirement for mankind oversight to take care of issues. Mechanical autonomy, then again IoRT, is a field of science that has been kept down the innovation of now is the ideal time. To finish it off, the speculation required to send mechanical technology-based arrangements is high.

The following are widened areas of usage of artificial intelligence-enabled IoT-based robotics in every sector of the world including manufacturing units, healthcare sectors, retail sectors, electronics gadgets, transportations, and many more as shown in Fig. 6.

Home and Buildings: Smart homes and buildings are equipped with many intelligent systems like a fire alarm, gas leakage systems, security management, monitoring systems, automatic lifts, and building alarms. Solar systems and water systems in the building are also apart of the intelligent system (Rai et al., 2021; Bamdale et al., 2019; Raj & Seamans, 2019). At present, during COVID-19, many smart home appliances are available for daily household works like mopping, cleaning, automatic chapatti maker, etc.

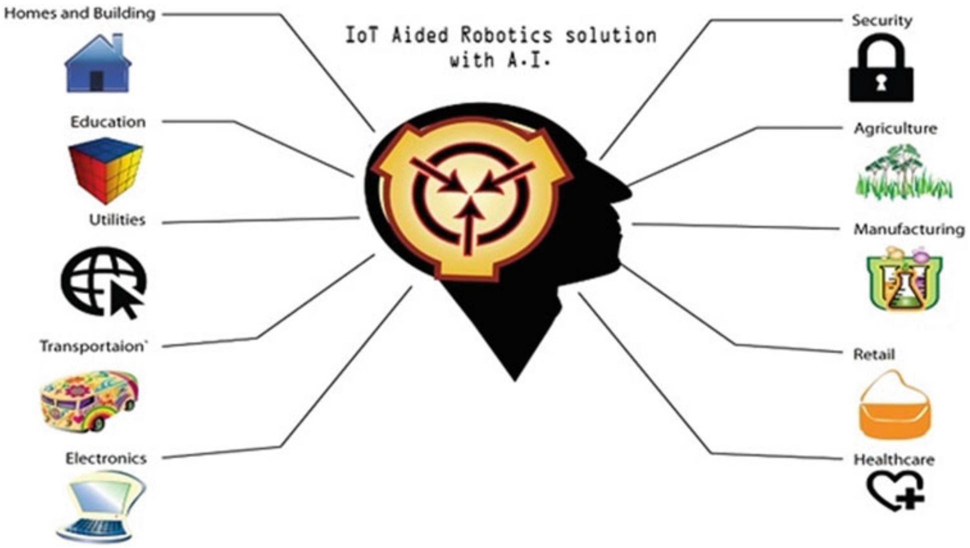


Fig. 6 IoT-aided Robotics solution in different sectors with AI

Healthcare applications: Bots in health care are typically understood in the literature and are broadly in practice in the current scenario (Lund, 2004; Leng & Mital, 1989; Bamdale et al., 2019; https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/a-robot-that-explains-its-actions). All these AI-based processes can be organized to offer support to disabled, senior citizen patients, and those with locomotor issues (Global Employment Institute Artificial Intelligence and Robotics and Their Impact on the Workplace, 2017). Observing and recording of medical equipment or insufficiency of any medical equipment can help to develop such systems so that there is no time wasted in observing and maintaining of the hospital and the doctors and the hospital staff can take care of even a large number of patients. R. Murphy, V. Gandudi, Texas A&M, and J. Adams (https://www.smithsonianmag.com/innovation/how-robots-are-on-front-lines-battle-against-covid-19-180974720) from Center for Robot-Assisted Search and Rescue presented a report that how intelligent and IoT-aided robots are helpful during COVID-19 in different countries at the different ground of reality as shown in Fig. 7. It states that during a disaster, robots do not replace people but it can also execute responsibilities that a person could not do or do safely, or help them to handle the increased workload. These intelligent and IoT-aided robots are teleported, empowering the medical personnel to apply their knowledge and concern to sick and isolated patients without taking risk of infections.

Industrial Applications and Personal Applications: IoT arrangements take care of a broad scope of issues in the industry from electrical matrix framework observing, temperature checking, power utilization, grease status, and so on (https://homepages.laas.fr/felix/publis-pdf/aicom13.pdf; Raj & Seamans, 2019). IoT applications are likewise frequently utilized in edge interruptions discovery frameworks at air terminals, railroad stations, and boat ports. Brilliant items involving the remote sensor arrange are utilized to empower mechanization, vitality observing, and control and reconnaissance framework (Jim, 2018).

Military Applications: The most widely recognized kind of mechanical military application would be the automatic aeronautical, ground, and submerged vehicle. These robots are used to cover territories which would regularly put the life of numerous officers in danger. Utilizing these, remote reconnaissance and assault can be done over pivotal vital zones. Internet of Things-supported bot applications can incorporate the co-appointment of brilliant articles with UAVs, UGVs, and UUVs (Hussain et al., 2009; Durisic et al., 2012; Wooden et al., 2010; Comte et al., 2012).

Rescue Applications: Robotic systems in recurred are utilized in search and salvage, where it is excessively risky or not truly feasible for salvage and help powers to spare individuals. IoT-assisted robotic applications can be utilized to arrange with alleviation and salvage powers on the ground to organize activities as per hazard and harm to the earth and afterward to send robot applications to perform a search, cleaning, and also the rescue operations on the field of disaster (Comte et al., 2012; Saha & Matsumoto, 2007).

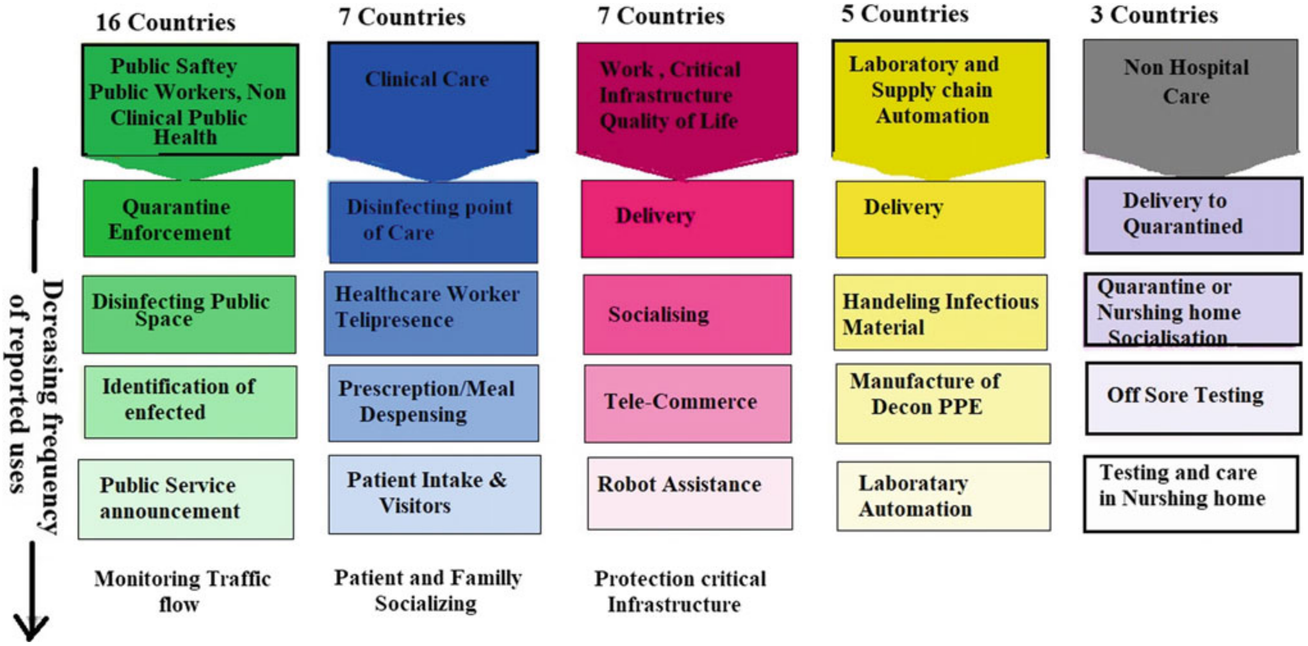


Fig. 7 Use of Smart and Intelligent Robots worldwide for COVID-19 as of April 2020 (https://www.smithsonianmag.com/innovation/how-robots-are-on-front-lines-battle-against-covid-19-180974720)

Intelligent Transportation System (ITS): It is progressive applications in which, without representing intelligence as such, goals to give advanced services relating to different modes of transportation and traffic management and empower various users to be informed and make safer, more coordinated, and "smarter" use of transport links (Intelligent Transportation System, 2017).

3.8 Challenges in AI-Based Robotics Development

Researchers in the field of artificial intelligence (AI) and Robotics-based Journal Science get a survey about the challenges in addressing to deliver highly robust and secure operations using AI-based robotics at considerable measure (Talwana & Hua, 2016; Silva et al., 2019; Islam et al., 2012; Biswas et al., 2014; Guizzo, 2011; Du et al., 2016; https:www.therobotreport.com/10-biggest-challenges-in-robotics; https://www.uipath.com/blog/solving-robotic-ai-challenges; https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade). Based on an online survey, the Journal of Science Robotics has stated that ten major challenges in this field will have to struggle with to make that reality in the next 5–10 years (Talwana & Hua, 2016; Da et al., 2019; Islam et al., 2012; Biswas et al., 2014; Guizzo, 2011; Du et al., 2016; https:www.therobotreport.com/10-biggest-challenges-in-robotics; https://www.uipath.com/blog/solving-robotic-ai-challenges; https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade). Researchers are rapidly moving in the direction of implementing mission-critical robotic operations, which will impact everyone's life in the coming days either employee, customer, and supplier, and all will be working together to deliver extraordinary competitive advantages (Stergiou et al., 2016,2018; Aazam et al., 2014; Yun & Yuxin, 2010; Wang et al., 2014; https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade). The robotics industry working with AI for smart robots with IoT enabled has numerous challenges, and this list is not comprehensive. Many of the challenges edge empowering technologies such as artificial intelligence (AI), perception, power sources, Internet on things, and machine learning.

Another challenge in IoT-aided intelligent robotics is human–robot interfacing and interaction for a real-time working environment (Bamdale et al., 2019). Artificial intelligence has many subdomains that can integrate with robotics for modeling humans and human cognitions, acquiring knowledge at human levels. AI-based robotics systems can work in saving lives and solving the world's hardest problems with some of their software and hardware challenges (Leng & Mital, 1989; Bamdale et al., 2019; Global Employment Institute Artificial Intelligence and Robotics and Their Impact on the Workplace, 2017; https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/a-robot-that-explains-its-actions; https://www.smithsonianmag.com/innovation/how-robots-are-on-front-lines-battle-against-covid-19-180974720). Figure 8 shows the most recent challenges in the field of IoT-aided robotics with AI-enabled systems.

Complex automated controller used robots enabled with intelligence and IoT are never simple to tune because of the intricate elements with idleness and regular frequencies changing with position and huge running payloads. It can be accepted that AI techniques should be made and enhanced to rearrange this procedure and to manage changes that consequence of automated wear after some period that can ever hope to see widespread dependable utilization of robots all over real life in the real world (Rai et al., 2021; Grieco et al., 2014; Talwana & Hua, 2016; Silva et al., 2019; Islam et al., 2012; Biswas et al., 2014; Guizzo, 2011; Du et al., 2016; https:www.therobotreport.com/10-biggest-challenges-in-robotics; https://www.uipath.com/blog/solving-robotic-ai-challenges; https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade). Figure 8 describes the 10 major areas of challenges in the field of robotics with AI and IoT.

New Material and Fabrication Schemes: Gears, motors, and actuators are essential to the present robots. Although some remarkable effort is already enforcing with artificial muscles and humanoid, soft robotics for medical work and assembly strategies by many researchers that will benefit for the next generation of self-directed robot developments, more researches are required for multifunctional and power-efficient robot's developments. But most of these improvements have been not easy to combine. Some multi-functional material and power-efficient requirement merger could allow more useful robot designs. Some or more researchers also work in the promising direction of component fabrication materials which can use merging things like sensing, movement, flexibility, energy harvesting, and storage units (Talwana & Hua, 2016; Silva et al., 2019; Islam et al., 2012; Biswas et al., 2014; Guizzo, 2011; Du et al., 2016; https:www.therobotreport.com/10-biggest-challenges-in-robotics; https://www.uipath.com/blog/solving-robotic-ai-challenges; https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade).

Creating bio-inspired robots: Robots motivated ordinarily are getting progressively basic in mechanical technology labs. The fundamental thought is to make robots that perform increasingly like the effective frameworks found in nature. In any case, the investigation says that the significant difficulties associated with this region have remained to a great extent unaltered for a long time—a battery to coordinate metabolic transformation, muscle-like actuators,

Fig. 8 10 biggest challenges in robotics that may have revolutions in 5–10 years. *Credit* Science Robotics

self-recuperating material, self-sufficiency in any condition, human-like recognition, and calculation and thinking (Talwana & Hua, 2016; Silva et al., 2019; Islam et al., 2012; Biswas et al., 2014; Guizzo, 2011; Du et al., 2016; https://www.therobotreport.com/10-biggest-challenges-in-robotics; https://www.uipath.com/blog/solving-robotic-ai-challenges; https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade).

Better power sources: Robots, ordinarily, are vitality wasteful. Improving battery life is a significant issue, particularly for automatons and portable robots. Fortunately, the expanded selection of these frameworks is prompting new battery innovations that are reasonable, sheltered, and longer-enduring (https://www.uipath.com/blog/solving-robotic-ai-challenges). Research is also conducted to improve eatable and disposable battery technology rather than already available technology like the nickel-metal hydride and lithium-ion.

Robot swarm's communication: Another challenge with robots and AI is communication between the robot swarms because robots are required to sense the environment as well as another robot in the swarm. They are required to communicate with the other robots, too, while acting independently.

Navigation and Exploration environments: A key use case for robots is investigating places where people cannot go, for example, the Remote Ocean, space, or fiasco zones. That implies they have to get skilled at investigating and exploring unmapped, frequently exceptionally scattered, and antagonistic conditions.

AI for Robotics: Profound learning has upset machines' capacity to perceive designs, however, that should be joined with model-based thinking to make versatile robots that can learn on the fly.

Other challenges with AI-enabled robots are brain–computer interfaces, social interaction, medical robotics, and robot ethics and security.

4 Conclusion and Future scope

In this chapter, research is enlightened regarding the prominent scientific and technological challenges area of IoT-aided robotics with specific reference of applications and some specific domain of implementation which can be supported by IoT-based robotics. The obstacle in developing an intelligent agent is an essential integration point of both fields: artificial intelligence and IoT-aided robotics. AI is playing very important and noticeable track in perception and planning for effective real-world problems and gives new research directions in the field of science and technology for providing efficient solutions. The chapter shows the development of simplest robots based on microcontroller to the more robust robots such as humanoids including controllers, programing, sensors, and intelligent systems, which can perform morphological features and intelligent tasks. These all are possible with merger of several technologies like cloud computing and IoT. The chapter also covers crossover domains with their solution and abilities, which provide researchers to explore more impact of systems.

References

https://www.therobotreport.com/10-biggest-challenges-in-robotics/.

https://www.uipath.com/blog/solving-robotic-ai-challenges.

https://singularityhub.com/2018/02/06/the-10-grand-challenges-facing-robotics-in-the-next-decade/.

https://tdwi.org/articles/2020/04/27/arch-all-smart-devices-and-coming-of-edge-computing.aspx.

https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/a-robot-that-explains-its-actions.

https://www.smithsonianmag.com/innovation/how-robots-are-on-front-lines-battle-against-covid-19-180974720.

https://homepages.laas.fr/felix/publis-pdf/aicom13.pdf.

Aazam, M., Khan, I., Alsaffar, A. A.., & Huh, E. (2014). Cloud of things: Integrating internet of things and cloud computing and the issues involved. In *Proceedings of 2014 11th international Bhurban conference on applied sciences & technology (IBCAST)* (pp. 414–419). Islamabad, Pakistan, 14th–18th January, 2014. https://doi.org/10.1109/IBCAST.2014.6778179.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.

Babatunde, O., & Al-Debagy, O. (2014). A comparative review of internet protocol version 4 (IPv4) and internet protocol version 6 (IPv6). *International Journal of Computer Trends and Technology (IJCTT), V13*(1), 10–13. ISSN: 2231-2803. Published by Seventh Sense. www.ijcttjournal.org.

Bamdale, R., Sahay, S., & Khandekar, V. (2019). Natural human robot interaction using artificial intelligence: A survey. In *2019 9th annual information technology, electromechanical engineering and microelectronics conference (IEMECON)* (pp. 297–302). Jaipur, India.https://doi.org/10.1109/IEMECONX.2019.8877044.

Bertelsen, O. W., & Bødker, S. (2003). *Activity theory in HCI models, theories, and frame works toward a multidisciplinary science* (pp. 291–324).

Biswas, A. R., & Giaffreda, R. (2014). IoT and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375–376). Seoul.https://doi.org/10.1109/WF-IoT.2014.6803194.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on mobile cloud computing* (pp. 13–16). MCC'12, ACM, New York, NY, USA. https://doi.org/10.1145/2342509.2342513.

Bo, Y., & Wang, H. (2011). The application of Cloud computing and the internet of things in agriculture and forestry. In *2011 International Joint Conference on Service Sciences (IJCSS)* (pp. 168–172). IEEE.

Chen, Y., & Hu, H. (2013). Internet of intelligent things and robot as a service. *Simulation Modelling Practice and Theory, 34*, 159–171. ISSN 1569-190X. https://doi.org/10.1016/j.simpat.2012.03.006.

Da Silva, D., Wang, Q., & Zhang, L. J. (2019). Correction to: Cloud computing—CLOUD 2019. In D. Da Silva, Q. Wang, L. J. Zhang (Eds.), *Cloud computing—CLOUD 2019. CLOUD 2019. Lecture Notes in Computer Science*, vol. 11513. Cham: Springer.

Durisic, M., Tafa, Z., Dimic, G., & Milutinovic, V. (2012). A survey of military applications of wireless sensor networks. In *2012 Mediterranean conference on embedded computing (MECO)* (pp. 196–199).

Du, Z., He, L., Chen, Y., Xiao, Y., Gao, P., & Wang, T. (2016). Robot cloud: Bridging the power of robotics and cloud computing. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2016.01.002.

Grieco, L. A., Rizzo, A., Colucci, S., Sicari, S., Piro, G., Di Paola, D., & Boggia, G. 2014. IoT-aided robotics applications: Technological implications, target domains and open issues. *Computer Communications, 54*, 32–47. ISSN 0140-3664. https://doi.org/10.1016/j.comcom.2014.07.013.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer System, 29*(7), 1645–1660.

Guizzo, E. (2011). Robots with their heads in the clouds. *IEEE Spectrum*

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Hussain, M. A., Khan, P., & Sup, K. K. (2009). WSN research activities for military application. In 11th *IEEE international conference on advanced communication technology* (pp. 271–274).

Islam, A., Hu, G., Tay, W. P., & Wen, Y. 2012. Cloud robotics: Architecture, challenges and applications. *IEEE Network, 26*(3), 21–28.

Intelligent Transportation Systems. (2017). https://en.wikipedia.org/wiki/Intelligenttransportationsystem. Accessed January 2, 2017.

IBA Global Employment Institute Artificial Intelligence and Robotics and Their Impact on the Workplace. (2017). Prepared by: Gerlind Wisskirchen Blandine Thibault Biacabe Ulrich Bormann Annemarie Muntz Gunda Niehaus Guillermo Jiménez Soler Beatrice von Brauchitsch.

Jim, T. (2018). A review of future and ethical perspectives of robotics and AI. *Frontiers in Robotics and AI, 4*, 75. https://doi.org/10.3389/frobt.2017.00075, https://www.frontiersin.org/article/10.3389/bfrobt.2017.0007.

Kaelbling, L. P. (1988). Artificial intelligence and robotics. In *Digest of Papers. COMPCON Spring 88 Thirty-Third IEEE computer society international conference* (pp. 59–61). San Francisco, CA, USA. https://doi.org/10.1109/CMPCON.1988.4828.

Kehoe, B., Patil, S., Abbeel, P., et al. (2015). A survey of research on cloud robotics and automation. *IEEE Transactions on Automation Science and Engineering, 12*(2), 398–409.

Kuo, A. M.-H. (2011). Opportunities and challenges of cloud computing to improve health care services. *Journal of Medical Internet Research, 13*(3).

Lazarescu, M. (2013). Design of a WSN platform for long-term environmental monitoring for IoT applications. *IEEE Journal of Emerging Selected Topics Circuits System, 3*(1), 45–54.

Le Comte, B., Sen Gupta, G., & Chew, M.-T. (2012). Distributed sensors for hazard detection in an urban search and rescue operation. In *IEEE international instrumentation and measurement technology conference (I2MTC)* (pp. 2385–2390).

Lekkala, K. K., & Mittal, V. K. (2015). Artificial intelligence for precision movement robot. In *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 378–383). Noida. https://doi.org/10.1109/SPIN.2015.7095321.

Leng, G. W., & Mital, D. P. (1989). A robotic system with AI. In *Fourth IEEE region 10 international conference TENCON* (pp. 999–1002). Bombay, India. https://doi.org/10.1109/TENCON.1989.177099.

Lund, H. H. (2004). Modern artificial intelligence for human-robot interaction. *Proceedings of the IEEE, 92*(11), 1821–1838. https://doi.org/10.1109/JPROC.2004.835362.

Mitton, N., Papavassiliou, S., Puliafito, A., & Trivedi, K. S. (2012). Combining cloud and sensors in a smart city environment. *EURASIP Journal of Wireless Communication Network, 2012*(1), 1–10.

Nayyar, A., Puri, V., Nguyen, N. G., & Le, D. N. (2018). Smart surveillance robot for real-time monitoring and control system in environment and industrial applications. In *Information systems design and intelligent applications* (pp. 229–243). Springer, Singapore.

Petrolo, R., Loscrì, V., & Mitton, N. (2014). Towards a smart city based on Cloud of Things. In *Proceedings of the 2014 ACM international workshop on wireless and mobile technologies for smart cities* (pp. 61–66). ACM.

Rai, A., Karatangi, S. V., Agarwal, R., & Prakash, O. (2021). *Smart sensors transforms healthcare system*. https://www.appleacademicpress.com/deep-learning-and-iot-in-healthcare-systems-paradigms-and-applications/9781771889322#bios.

Raj, M., & Seamans, R. (2019). Primer on artificial intelligence and robotics. *Journal of Organization Design, 8,* 11. https://doi.org/10.1186/s41469-019-0050-0.

Rao, B. P., Saluia, P., Sharma, N., Mittal, A., & Sharma, S. V. (2012). Cloud computing for internet of things and sensing based applications. In *2012 sixth international conference on sensing technology (ICST)* (pp. 374–380). IEEE.

Ray, P. P. 2016. Internet of robotic things: Concept, technologies, and challenges. *IEEE Access, 4,* 9489–9500. sma.com/iot/iot-opportunities-impacts/.

Roy Chowdhury, A. (2017). IoT and robotics: A synergy. *Peer Journal, 5,* e2760v1. https://doi.org/10.7287/peerj.preprints.2760.

Saha, S., & Matsumoto, M. (2007). A framework for disaster management system and WSN protocol for rescue operation. In *TENCON IEEE region 10 conference* (p. 14).

Schlussel, K. (1983). Robotics and artificial intelligence across the Atlantic and Pacific. In *IEEE Transactions on Industrial Electronics, IE-30*(3), 244–251. https://doi.org/10.1109/TIE.1983.356735.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2016). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2016.11.031.

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy and efficiency of sustainable cloud computing for big data and IoT. *Sustainable Computing: Informatics and Systems*. https://doi.org/10.1016/j.suscom.2018.06.003.

Talwana, J. C., & H. J. Hua. (2016). Smart world of internet of things (IoT) and its security concerns. In *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 240–245). Chengdu.

Tsai, W. T., Paul, R., Xiao, B., Cao, Z., & Chen, Y. (2005). PSML-S: A process specification and modeling language for service oriented computing. In *The 9th IASTED international conference on software engineering and applications (SEA)* (pp. 160–167). Phoenix, November 2005.

Verma, A., & Kumar, S. (2018). Cognitive robotics in artificial intelligence. In *2018 8th international conference on cloud computing, data science & engineering (confluence)* (pp. 65–70). Noida. https://doi.org/10.1109/CONFLUENCE.2018.8442725.

Vermesan, O., Bröring, A., Tragos, E., et al. 2017. Internet of robotic things: Converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT platforms. In O. Vermesan, & J. Bacquet (Eds.), *Cognitive hyperconnected digital transformation: Internet of things intelligence evolution* (pp. 1–35). Norway, Belgium: River Publishers Series.

Wang, C., Bi, Z., & Xu, L. D. (2014). Iot and cloud computing in automation of assembly modeling systems. *IEEE Transactions Industrial Informatics, 10*(2), 1426–1434.

Wooden, D., Malchano, M., Blankespoor, K., Howardy, A., Rizzi, A., & Raibert, M. (2010). Autonomous navigation for bigdog. In *IEEE International conference on robotics and automation (ICRA)* (pp. 4736–4741).

Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2013). Transition from IPv4 to IPv6: A state-of-the-art survey. *IEEE Communications Surveys & Tutorials, 15*(3), 1407–1424. https://doi.org/10.1109/SURV.2012.110112.00200.

Xiao, Y., Simoens, P., Pillai, P., Ha, K., & Satyanarayanan, M. (2013). Lowering the barriers to large-scale mobile crowd sensing. In *Proceedings of the 14th workshop on mobile computing systems and applications* (pp. 9:1–9:6). HotMobile'13, ACM, New York, NY, USA. https://doi.org/10.1145/2444776.2444789.

Yun, M., & Yuxin, B. (2010). Research on the architecture and key technology of internet of things (IoT) applied on smart grid. In *2010 international conference on advances in energy engineering (ICAEE)* (pp. 69–72). IEEE.

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). *Sensing as a service and big data*. arXiv:1301.0159.

Convergence of IoT and CPS in Robotics

Parita Jain, Puneet Kumar Aggarwal, Poorvi Chaudhary, Kshirja Makar, Jaya Mehta, and Riya Garg

Abstract

With the expeditious growth of technology, robotics seems to be the new literature of the world. The idea of digitalizing machines, automation and computers is making robotics to grow at a faster velocity. In accordance with the Internet of things (IoT) and cyber-physical system (CPS), a new hypothesis of robotics is emerging. IoT cooperates with devices through wireless or wired medium to create new applications and gadgets to reach specific goals. If CPS is the viaduct for the emerging advancement of technology, then IoT is an upright for the technology. There are numerous amounts of fields where convergence is evident, such as driverless cars, decision-making, agriculture and many more. This chapter focuses on how two different aspects IoT and CPS converge together in the robotics industry making it more efficient and pleasing to adapt by other organizations, institutions, etc.

Keywords

Applications of CPS and IoT • Collation of CPS and IoT • Cyber-physical system (CPS) • Internet of things (IoT) • Internet of robotics things (IoRT) • Robotics

1 Introduction

If the world today is beautiful then with robotics it will be remarkable. Robotics can be seen as the science of operating, designing, constructing robots and computers for the purpose of processing information and having control over the system, for delivering the desired results. The following chapter brings limelight to the intensifying industry of robotics with the help of technologies like cyber-physical system (CPS) and Internet of things (IoT). Cyber-physical systems can be portrayed as an interconnectivity between the cyber and the physical world. Internet of things (IoT) is the field based on the connectivity of multiple devices, these when combined with machine learning (ML), artificial intelligence (AI) and data mining techniques can create wonders.

Time is changing constantly and so is the technology, new expressions of CPS and IoT in robotics are making it more user friendly and complex. The facilities and luxury which are steadily appearing from the ultimate relationship of CPS and IoT are accelerating services, economy, telecommunication, businesses, etc., by ignoring every extremity coming in the way. This combination gave the inspiration for the construction and development of Internet of robotic things (IoRT). IoRT is basically a combination of various technologies such as cloud computing, machine learning, artificial intelligence and Internet of things. It refers to the concept in which the sensor information is integrated and refined in order to regulate and handle the objects in the real world. In the further sections of the chapter, a detailed analysis of IoRT, its abilities and usage in day-to-day activities is discussed.

Everything is now getting available in just a click. Devices that are associated with the Internet are facing a threshold of advancement. Researchers, organizations and institutions are adapting to changes. Robots are their new recommendation because they provide them real-time solutions. With the stupendous enhancement of CPS and IoT, a

P. Jain (✉)
KIET Group of Institutions, Ghaziabad, UP, India
e-mail: paritajain23@gmail.com

P. K. Aggarwal
ABES Engineering College, Ghaziabad, UP, India

P. Chaudhary · K. Makar · J. Mehta · R. Garg
HMRITM, Delhi, India

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_2

cheap processor can now turn into a complex robot. This chapter also includes how IoT is responsible for sensing, communication and decision-making of a robot whereas CPS is responsible for all the physical aspects of a robot. It also provides an assessment of all the outstanding and worst possible aspects of IoT and CPS which took place in a robotics.

Our world is witnessing some extravagant applications of convergence of IoT and CPS in robotics starting from Sophia—the robot to the robot snake and more are about to come. We are stepping into a time where everything is so evolved, robot is there to help us, make our work easier and boost our world with the frequent number of resources. The whole point behind this chapter is to make people aware of all the available opportunities we are surrounded within the robotics industry and how a simple robot can be made a new sign of brilliance with the involvement of CPS and IoT.

The rest of the chapter is organized into different sections. Section 2 discusses about the concept of IoT and how it works. In Sect. 3, the convergence between the IoT and robotics is discussed which defines IoRT. Then, various applications of IoT are discussed and described in Sect. 4. Section 5 discusses the different applications of convergence of IoT and robotics. The concept of cyber-physical system (CPS) is discussed in Sect. 6 of the chapter. The different complex problems and its solution to CPS are described in Sect. 7. Then, Sect. 8 defines the applications of convergence of CPS and robotics and Sect. 9 describes the collation of CPS and IoT. Then in Sect. 10, conclusions are drawn from the chapter, including the future scope. Finally, references at last.

2 Internet of Things (IoT)

As the world is moving towards technology IoT is a subject that cannot be ignored. IoT can be referred to as a system that connects various digital and computer devices and makes human–computer interaction much easier. It is a term that creates a notion that all the IoT devices have the capability to inspect and collect the information from the real world and pass it on to the Internet that is a virtual world where it can be used positively for other applications and interesting projects. The concept of “smart devices” or “smart home” has come into existence because of IoT. All the appliances that we use today or will be using in the future (such as lighting fixtures, thermostats, home security systems and cameras) that support one or more common ecosystems or environments use IoT in some direct or indirect way (Atzori et al., 2010). Today each and every common person in the world is familiar with the word IoT because it is making our life much easier and comfortable.

2.1 History of IoT

It all began with a network of devices called smart devices in early 1982. The first device to be connected to the Internet was a Coca-Cola vending machine. This machine could tell that if the newly loaded drinks were cold or not. In 1994, Reza Raji explained “From small packets of data to large pieces of information if combined can robotize everything small house applications to entire industrial applications”. The major achievement was received when Bill Joy visualized communication among various devices and hence forming a network which he called “Six Webs” framework and was represented at World Economic Forum in 1999. The term “Internet of Things” was introduced by Kevin Ashton literally meaning “Internet FOR Things” in 1999 during his work at Procter & Gamble. Then he was working on a project and to grab the attention of the senior management towards a new technology RIFD he introduced this term. He suspected that this area can be successfully implemented by the use of computers (Minerva et al., 2015; Ashton, 2009).

The first definition of IoT was “the objects being connected to the Internet more than humans”. The major leading force behind the Internet of things is metal–oxide–semiconductor field-effect transistor (MOSFET). MOSFET played a major role in building of electronics, which includes computers, smart phones, laptops, etc.

The term “Internet of things” is 16 years old, but the concept was introduced a long time ago. Then in the past it was called as “embedded Internet” or “pervasive computing”. Originally this term gained popularity in summer 2010. In this year China announced that “Internet of things” would be their prime concern in next Five Year Plan. In 2011 Gartner, the market research company invented something famous which made use of “IoT”. In 2012, the biggest and most popular European conference was based on the topic “IoT”, also in the same year the popular technology magazine worldwide named Forbes also released an article on “IoT”. This term reached market and to common people’s acquaintance by 2014.

2.2 How IoT Works

It consists of a well-connected system made up of smart devices such as sensors, communication software and hardware and some processors to act appropriately on the data received from their ecosystems. These smart devices share the data among them that they have collected by connecting to a main device also called “IoT gateway” where the data collected is further sent to be analysed. These devices are related only by the means of information or data that is shared between them. The specialty of these smart

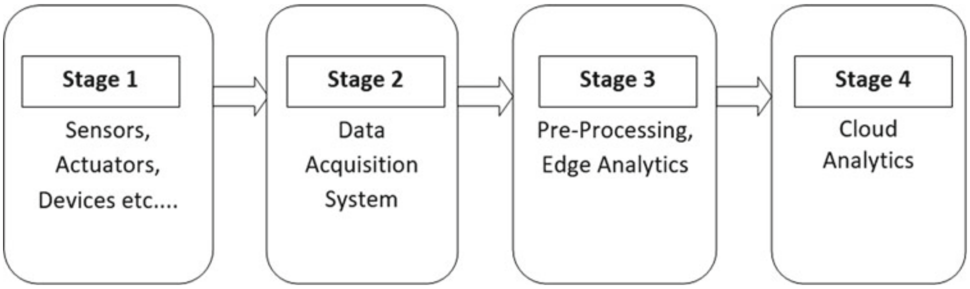


Fig. 1 Four stages of IoT architecture

devices is that they are designed in such a way that they not require manual aid to perform their functions, though humans can intervene to assure their proper working such as providing the instructions, managing the settings and accessing the data. They use various connectivity, networking and communication protocols to successfully form the applications that we are using today. The most important thing about these devices is that these devices provide the ideal service as a system not as an independent individual that is they cannot work individually; they need a connected system and network in order to perform functions (Koreshoff et al., 2013; Li et al., 2015).

2.3 Importance of IoT

IoT is especially important for large-scale businesses where all the work cannot be handled manually. Also, it costs much less than the human labour and is more efficient. Hence, it reduces time, cost and effort.

Apart from setting large-scale businesses it is used to manage already set up businesses as it helps to look into the smallest details, for example how the systems actually work, whether all the things are working as expected, the growth rate, the problems in the system, logistic operations, etc. It also helps in effective decision-making and generates more revenue (Whitmore et al., 2015). It can monitor the changes happening in the surrounding environment with the help of sensors which makes it more reliable in fields like agriculture where the work of the farmer is reduced as it monitors all the factors such as rainfall, humidity and temperature. Similarly, in buildings, houses, etc., it can monitor electrical and mechanical systems as well. Hence, IoT can be utilized in all the sectors of industry.

2.4 Architecture of IoT

IoT is not only the technology that consists of devices that connect humans and Internet. But it is actually the technology that enables the building of complete systems that are capable of sensing information from the human world and performing all the functions without human intervention. Actually, this system is quite complicated to be implemented if it is not well built (Sarma et al., 2000; Ibarra-Esquer et al., 2017). Therefore, the architecture of IoT plays an important role in simplifying the implementation part of the system. This also reduces the number of sources invested in the process. Understanding the architecture makes us understand what the concept of IoT actually means. IoT architecture is the system that contains a number of elements: sensors, protocols, actuators, cloud services and layers.

The three IoT architecture layers are:

1. IoT device layer
2. IoT getaway layer
3. IoT platform layer

Considering these layers of IoT is very important as they are a very crucial part of the architecture. Besides these layers IoT architecture includes functionality, scalability, availability and maintainability. The four main stages of IoT architecture are described in Fig. 1:

Stage 1: Sensors and Actuators:

The ability of sensors is to recognize and convert the information available in the real world for analysis. This stage is important to start by actually collecting the information. Actuators are even more advanced and better than sensors as they are able to intervene into the reality and adjust the information accordingly. They generally control the physical environment, for example they are capable to switch off the lights and fans, etc.

Stage 2: Internet Getaways and Data Acquisition Systems:

The data from the sensors is now needed to be sorted, aggregated and converted into digital signals. Data acquisition systems are required in order to perform these aggregations and conversions. DAS work by connecting to sensors while Internet gateways connect to Wi-Fi and wired LANs for further processing.

Stage 3: Edge IT:

Now the data is prepared to send into the computer world. Edge IT here plays a vital role in pre-processing and analysing the data one last them before it is transferred into IT world. This stage connects IoT to the IT world and establishes an indirect connection between human and computer world too.

Stage 4: Data Centre and Cloud:

This is actually the management stage that helps in storing and managing the already analysed data. The main task is visualization and management. Here, the data is further sent to cloud-based systems. After this stage the process again repeats itself.

3 Convergence of IoT and Robotics

By hearing the term robotics, one generally imagines a typical machine, like robots, that is seen in movies like Terminator, etc. But actually "robotics" is a more technical term which is specially an engineering domain offering help and solutions to various industries. If we see from the point of view of Internet of things robots are extremely smart devices as compared to others because of the extensive use of artificial intelligence. Robotic systems are inbuilt machines originally designed to reduce human labour, but these robots are designed to perform intensive labour work with a small set of technology to act upon their surrounding environment conditions, while machine learning and IoT allow these machines to function in decision-making and learning algorithms make machines smarter and reduce the physical work. IoT is used to provide robots with a wide range of awareness according to situations that lead to better performance of tasks. Today, IoT is being recognized by words like autonomous vehicles and drones, due to which robotics and Internet of things are becoming more and more converged.

IoT-robotics convergence is now also called as Internet of robotic things (IoRT). IoT and robotics initial objectives were sensing, tracking and monitoring the extensive information and then later on were developing action and interaction and autonomous behaviour. IoRT is now more focused on M2M communication and intelligent data processing.

IoT and robotics convergence leads to the formation of a networked robot. A "networked robot" is a connected robotic device connected to a communications network such as the Internet or LAN. The network could be wired or wireless and based on any of a variety of protocols. The two subclasses of networked robot are:

- *Tele-operated robots* where human send commands and receive feedback via the network. These systems support research, education and public awareness by making valuable resources accessible to broad audiences.
- *Autonomous robots* where robots and sensor exchange data via the network without human intervention. In these kinds of systems, the sensor network has even more effective sensing range of the robots, allowing them to communicate with each other over long distances to coordinate their activity. The robots, in turn can deploy, repair and maintain the sensor network to increase its longevity. Networked robots need wireless networks for sharing data among other robots, and to communicate with one-other and powerful workstations are used for creation of globally consistent maps of the robot's environment.

The evolution of these systems has now reached the real consumer market, for example support remote meetings and as telepresence healthcare tools. Some of the signs of this convergence are evident and can be seen with examples like driverless cars. The final aim of this car is a connected device/robot that is smart enough to perform some basic drive functions on its own without the need of any human. More examples of Internet of robotic things are network robot systems or robot ecologies and cloud robotics.

Number of fields is there where we can see examples of this convergence, agriculture where drones are used for monitoring environmental conditions and soil conditions. This practice is most commonly seen in Japan.

3.1 Basic Abilities of IoRT

The basic abilities of IoRT make it more special as it merges the features of both IoT and robotics together. These abilities can be defined as:

(i) *Perception Ability*: The special sensor and data analytics technologies from the IoT can clearly provide robots with a wider range compared to local, sensing, in terms of space, time and type of information. A key challenge of perception in an IoRT environment is that the environmental inspections of the IoRT entities are randomly and temporally distributed. So, there must be some techniques that must be put in place to allow robots to query these distributed data which is done by IoT by using local database in each entity in order to organize the random distributed data.

A key component of IoRT robots is that the perception ability is by getting knowledge of their own location, which includes the ability to build or update models of their own environment. Despite this achievement, self-localization is a problem in highly indoor environments.

(ii) *Motion Ability*: The capacity to move is one of the fundamental special values of robots in IoRT systems. While mechanical design is the major factor in determining the internal effectiveness of robot movement, IoT connectivity can assist mobile robots by helping them to control automatic doors and elevators. IoT technology services and M2M and networking protocols can facilitate distributed robot control architectures in large-scale applications, for example last mile delivery, precision agriculture and environmental monitoring. These in turn make the robot to act as a mobile sensor. It has applications in communication infrastructure these robots are used to maintain the communication between the devices

(iii) *Manipulation Ability*: Robots can grasp, lift, hold and move objects with the help of their end effectors, but they can do this by touching the objects. Once the robot has detected the relevant features of an object, like its position and contours, then the factors are calculated by applying inverse kinematics. IoT adds a value in the accession of the object features, in that are not visible with the robot's sensors, but surely have an impact on the grasping procedure, such as the distribution of mass which makes it possible to accurately determine the position before even touching the object.

(iv) *Interaction Ability*: Robot has the ability to interact physically, cognitively and socially either with users, other robots or other systems around it. IoT technologies can simplify and increase human–robot interaction at functional and social levels

Functional pervasive IoT sensors can make the interaction more vigorous. Natural language instructions are a desirable way to instruct robots, especially for the users who are not well versed with technology. Gestures or actions are another effective way to command robots, for instance, by pointing to objects. But these are the methods which require a lot of effort and time. The integration with IoT sensors can improve this interaction by measuring physiological signals, i.e. by measuring heart rate, etc. Tele-interaction is the western way of interaction which is only possible due to IoT technology. It is specially used in health care. IoRT robots are used to monitor the diabetes of a patient by checking the glucose sensor.

(v) *Configurability*: This refers to the ability of a robotic system to be configured to perform a given task or reconfigured to perform completely new and different task. This feature is most prominent in the domains of logistic computing and of advanced manufacturing, where a fast reaction to disturbance is needed, along with flexible adaptation to varying environments and objectives. Configurability when coupled with the decision-making capability to lead to the capacity of a system to self-configure. Self-configuration is especially challenging in an IoRT system because the configuration algorithms consider both the digital interactions and physical interactions through the real world. The "PEIS Ecology" structure includes algorithms for the self-configuration which is only possible for a IoRT robot.

3.2 IoT Robotics Software

The software required to run a robot can be classified into four levels of functionality. Each level has different characteristics with respect to timing, power demands and means to distribute the level over different computational units.

Level 1: The first and lowest level covers everything related to establishing an access to the hardware. This includes the operating system (OS), various services like tasks, murexes, hardware abstraction devices like timers, UART, PWM and various drivers for low-level interaction with the IT architectural sensors and actuators. At this level, all the functions are considered non-periodically and very low dormancy. Because of the direct interaction with the hardware unit, this level is stable and firm for a specific computing unit and hence cannot be distributed. The demands for processing power depend naturally on the number of sensors/actuators that are handled by this level.

Level 2: The second level of this software locates the periodically functioning and low-level control algorithms. Different controllers and various sensors (ranging from simple, average to sophisticated filters) are used in data handling algorithms. The algorithms for the mobility of the robot's arms and legs are also implemented here. The timing requirements at this level are quite fixed and rigid, for example motor controllers run with periods as low as 100s of nanoseconds, but there are some which ranges from 10s of microseconds to 100s of milliseconds. But the usage of fast running control loops is not preferable so it is compulsory to distribute sensor data aggregation and fusion over numerous nodes, therefore making this level partly distributable.

Level 3: This level involves trajectory planning and obstacle avoidance. This requires the robot to maintain a special focus on its environment. Depending on the complexity of the environment and the model, this can require a huge amount of memory and power. This level runs on simultaneous localization and mapping (SLAM) algorithms. These algorithms can be carried out flexibly at any point of time. This makes sure that the robot can be turned into a safe state at any point of time, thus saving it from collisions and or unnecessary failures.

Level 4: The highest level of robot software aims over mission and task control. The control periods on this level are rough, ranging typically from minutes upwards to days and months. In this level control software is being focused around the centralized control unit.

The software runs on forced IoT device and shares the same characteristics as Level 1. The timing completely depends on the actual and practical cases and can range from 100s of milliseconds to minutes and hours depending on the usage. In contrary to robotics software, the actual software is however distributed by default. Some of the applications can be implemented on Class 0 devices. Class 1 devices are considered the minimum when there is full Internet connectivity and security.

The communication between Levels 1 and 2 can be described as simple data flow, in which data is required to be sent and retrieved at a fixed periodic rate. The priority is always given to the newest data. Data loss is acceptable, but only to a certain extent because greater is the data loss more is the chances of the robot to stop functioning. The communication between Levels 2 and 3 is also referred to a data flow, but with potentially lesser requirements and complications as data exchanges is expected to occur at lower data rate. The communications between Levels 3 and 4 characteristics are more diverse. This level can introduce a service called request–response pattern where the data is only flowed when required, allowing only the certain amount that is actually needed.

3.3 IoT Robotics Communication

The robotic applications connect to some form of messaging system which actually benefits them in communication. This allows nodes to be installed on different computing units. So, if the computing system's power is exceeded the limit, these nodes automatically move in the outside environment without any modification required. But releasing nodes in external environment opens a new set of problems such as messages are facing data loss, jitter, extended delays and so on. Considering these limitations, the IoT robotics system of communication uses algorithms in order to overcome this set of issues.

In robotics, libraries like ROS or ZeroMQ are installed which provide messaging structures built exactly according to the needs of robotics applications, providing suitable conditions like low-delay data streams as well as reliable data exchanges. But these libraries need underlying OS support to function and are not designed for embedded environments, thus making it not appropriate to run them on constrained devices. The IoT domain has lately introduced much reliable efforts, bringing the Internet protocol pack into low-power and low-cost hardware which are the ideal requirements. IoT uses typically two types of communication patterns that are: request–response and publish-subscribe.

The most prominent protocols of IoT defined in this space include IPv6 and 6LoWPAN, MQTT-SN, CoAP, etc. To diminish the impact of unreliable IoT communication, two main approaches are needed to be explored. Smarter QoS mechanisms which are yet-to-be-defined and the adaptable robotics algorithms.

4 Applications of IoT

It can be used in almost all the fields like educational system, railways, airports, bus stand for display notifications and many more. Some of the applications are described as (Nayyar et al., 2017; Solanki & Nayyar, 2019; Batth et al., 2018):

(i) *Smart Cities*:

- Monitoring of parking areas availability in the city. The maturing of IoT has profoundly affected the commencement of the technology in terms of smart parking. From parking splotches to real-time parking maps, the infusion of IoT has availed everything further accelerated and effortless. Travelling becomes easier when solace is intricate. Incorporation of IoT platforms has upgraded the level of magnificence.
- Monitoring of vehicles and pedestrians to optimize driving and walking routes. Safety is predominant, especially when it is just a click away. IoT platform has sanctioned trackers or applications which can allow users to supervise the circumstances on roads. Real-time monitoring of driving can reduce the life risks exceedingly.
- Intelligent highways that warn, according to climate conditions and unexpected events like accidents or traffic jams. The census of accidents reveals that the supreme number of accidents takes place on highways. With the assimilation of IoT platform's diverse sensors, equipment can be used to prevent the situation. It can be taken into account for traffic management. Alerts can be convoluted for efficient driving on the Highways.

(ii) *Smart Agriculture*:

- Monitoring soil moisture and its quality. This ensures the maintenance of nutrients in soil and thus increases the agricultural production as the soil is the major factor responsible for agricultural growth. Monitoring of the soil is the major issue faced by the farmers as it requires constant care, but introduction of IoT makes it much simpler and efficient as well.
- The study of weather conditions in fields to forecast formation like rain, drought, snow or wind changes. Climate plays a major role in farming and the growth of crops. Inappropriate knowledge of weather forecast can lead to deterioration of both quality as well as quantity of crops. IoT allows real-time monitoring of weather conditions with the help of the sensors placed on the farms.

Sometimes these sensors also inspect the condition of the crops and the environmental conditions, thus making it easy for the farmers to decide which crops to grow in which season.

- It also helps in control of humidity and temperature levels in crops to prevent fungus and other microbial contaminants. It brings more precision or accuracy to the farming. Monitoring of different factors in farms like vehicles, tools utilized, weather conditions, soil nutrients and other important factors leads to an increment in the accuracy in farming which in turn assures good quality as well as quality of crops. This also allows the farmers to make quick and correct decisions. This also ensures profit in terms of the investment made.

(iii) *Smart Homes*:

- Automatic switching on and off appliances like fans, lights, etc., is done to save energy and to reduce the risk of hazards or accidents. For example, it detects the water or gas leakage within the house with the help of sensors and then the IoT ecosystem is altered and automatically the home appliance is turned off. All this process of detecting as well as taking the required action is completed by the IoT system on its own which makes the home even smarter.
- Detection of windows and door openings to prevent intruders is done, which increases the security of the home and its members with the help of security cameras, and other sensors which notify the user if anything goes wrong or unexpected. Other than this, it can also detect smoke. The smoke detectors allow the sensors to create a wireless network and connect the system to an app so that the user has all the updates of what is going on even when he is not in the house. Thus, if the smart home does not have any caretaker, then an IoT-based smart home can take care of itself.

(iv) *Medical Fields*:

- Monitoring of conditions of patients in hospitals can be done easily. The healthcare sector has unleashed the ultimate remedy for patients' safety and health with their collaboration with IoT. It has become further straightforward to store the data of patients more dynamically rather than maintaining columns on pages. With the familiarity of these devices' patients can be attended with more convenience and peace.
- Also, monitoring and controlling of conditions inside freezers for storing medicines and vaccines can be done easily. Pharmacy availability on a click has reformulated the circumstances to a further extension of proficiency. From applications of medicines providers to the results of tests, the evolution has been brisk and successful. Certain requisitions for hospital equipment, pumps, machines, etc., are now available. These devices keep a track of hospital requirements so that every patient should get the finest treatment.

5 Applications of Convergence of IoT and Robotics

The list applications of IoT are growing and will be growing as technology evolves in the future. In the years ahead, IoT will be collaborating with artificial intelligence to solve complex issues by providing smart solutions. Below are described some of the applications which one can see in the stream of robotics (National Science Foundation; Woodside & Sood, 2016).

(i) *Health care*:

One can see the applications of IoT integrated with robotics in varying fields, one of these fields include health care and human well-being. The medical centres and hospitals across the globe be it private or public are trying to modernize the services by accepting digitalization. This makes the organization to collect more data regarding the patient's medical conditions and history. The data is then used to collaborate the medical field with the robotic environment. The combined power of IoT with that of robotics has the potential to create a brighter future of the healthcare sector; tech giants like Samsung are ready to invest in the same. The vision is to make IoT sensors that can arrange video calls with doctors in case they are unable to visit a healthcare centre and provide them with home delivery of medicines, having sensors to check on a person's physical health and stress levels.

Through this the increasing demand of healthcare workers and upgradation of healthcare facilities can simultaneously be executed for the citizens. There are countries that are supporting the human support robots (HSRs), and companies like Toyota and Honda are engaged in the work. The demand seems to increase in the upcoming decades rapidly, especially in countries which face a shortfall in the number of like that of Japan. They perform simple tasks like helping people to get into bed, wake them up, reminding them to have their medicines, give them emotional support for those who lack regular human contact. Other examples include Surgical Robots and Hospital robots and this is possible due to IoT applications.

(ii) *Industry*:

The introduction of IoT and robotics working together is a crucial part of industrial robotics, which was once having unadvanced machines, but now these machines can handle the tasks with more efficiency. The industrial robotics is going to see even more intelligent robots to decrease human effort they will rely for data on IoT applications.

Amazon's warehouses have collaborated the potential of IoT with that of robots and machines and due to communicative benefits from IoT the collaboration becomes a huge success. These robots read the stickers which have barcodes on them present on the floor and navigate themselves and further fulfil the command of packaging and picking orders. The firm of robotics ABB is having the concept of using connected sensors index the concept of predictive maintenance, to make sure the parts get repaired before the stop functioning.

(iii) *Military*:

The perspective of urban warfare has changed now and the countries are trying their best to save lives, but still not stepping back from dominance issues. The solution comes from the field of IoT and robotics, also known as Internet of military things (IoMT) which include human-wearable biometrics, intelligent robots for battle field, use of sensors in the battlefield. US Army research laboratory has initiated projects to develop IoT and robots to achieve gains in the battlefield.

IoT applications are being more capable of supplying data to the field of robots to capably find their way to achieve the main goals, there robots will grow up to make new room for development and will help in economic growth.

(iv) *Farming*:

Farming in urban areas with the help of IoT applications is known as smart farming. The farmers are the one who works very hard to feed us with food, life depends on them for survival; this area can receive great help with IoT added robots. Smart farming mainly aims to provide help by sensing the crops need of water, manure, when the crop is ready to harvest, it is a harvest and lot more. This technology has the potential to eliminate extra labour and the task becomes fast yet easy.

6 CPS—Cyber-Physical Systems

As the term suggests, CPS—cyber-physical systems is basically a correlation between the cyber and the physical world. It is all about their intersection and not about their fusion. It has various concepts and prototypes that have been designed by taking reference from almost all engineering branches such as mechanical, environmental, civil, electrical, biomedical, chemical, and aeronautical and computer science. But the prototypes could not be combined easily; therefore, CPS has its own disciplinary rules and techniques (Lee, 2006; IEEE Technical Committee on Cyber-Physical Systems).

So, CPS—cyber-physical systems first came into picture around 2006 and was devised by "Dr. Helen Gill- a program director", at National Science Foundation Directorate for Computer and Information Science and Engineering (CISE) Division of Computer and Systems (CNS), USA. While we try to link CPS with "cyberspace", we must not get confused with "cyberspace" and "cyber-physical system" as they both are independent of the each other. Also, they have the same origin, that is, "cybernetics"—which was invented by Norbert Wiener around 1948. Mr. Wiener, a mathematician, influenced the control system theory completely. He proposed his facts regarding cybernetics as the convergence of physical operations, calculation and communication despite of being completely unknown to the digital networks. As the time passed by, CPS marked a tremendous growth in its research worldwide, that is, starting from just 35 articles in the year 2006 to nearly around 1000 articles in the year 2017. Moreover, the curiosity for knowing about the same increased over the years (Lee, 2010; Shi et al., 2011; National Institute of Standards and Technology, 2013).

Now, if one talks about CPS, gathering information regarding its components individually will be quite unfair. Therefore, the combination of the two is required to be studied in deep. This road map to CPS is important to be understood as a junction of computers, hardware and software, and physical processes.

CPS is the short for cyber-physical systems. These systems are refined yet safe and secured networked system that constitutes of sensors, control systems and processors already embedded in it. It is specially designed to make sure of the proper interaction and sensing of physical systems. CPS has administered an antidote by making less use of hardware and increasing the use of software enabled services. It is capable of decision-making and interaction with machines and human. A standard CPS consists of the following components (Rajkumar et al., 2010; Kim & Kumar, 2012; Sanislav & Miclea, 2012; Horvath & Gerritsen, 2012; National Research Council, 1995; Pallás-Areny & Webster, 2001):

- *Physical Components*: It includes hardware systems and processes that have been emerged from mechanical, electrical, electronic, hydraulic, pneumatic systems and many more.
- *Software Components*: This component generally looks after the logical portion that is required for a system to work such as algorithms, various decision-making techniques in accordance with the input provided to the system.

- *Communication*: This component handles the connectivity between the hardware and software among each other and to the others devices, therefore, swapping pieces of information over a network.

The various features of CPS are as follows:

- *Reflexible System*: This feature paints a picture of CPS being a responsive and reflexive system. This is evident from the fact that it endlessly interacts with the ecosystem at a rate bounded by that ecosystem.
- *Combined System*: The cyber-physical system exhibits both the continuous as well as discrete or distinct features at the same time. In other words, CPS constitute of analog and digital system simultaneously. This makes the system highly flexible.
- *Devotion Towards Some Applications*: This feature has been strange yet astonishing as it enhances the de-emphasis of resources. This system needs maximum efficient user interface.
- *Robust System*: CPS accommodates the following, one, the variation in the ecosystem, second, change in the total of perceived and substituted data and third, runtime change of the requirements.

Since the cooperation with the devices is done through either wired or wireless medium for the creation of new applications and gadgets to reach specific goals and desired services, mainly wireless communication technology is used by CPS. There are four distinct types of communication:

- Human-to-human communication
- Human-to-machine communication
- Machine-to-human communication
- Machine-to-machine communication

Implementation of CPS cannot happen without M2M communication. It is a vital permit for a CPS to work. Machine-to-machine (M2M) is a means of communication of various sensors, machines, robots, etc., without interference of humans.

6.1 Swarm Intelligence and Robotics

A further advancement in the field of artificial intelligence (AI), that is, swarm intelligence has completely transformed robotics adding features of communication and behavioural interaction not only among the robots but with the ecosystem as well. These special types of robots exhibit the following characteristics:

- Integration of different mindsets, rules and ideation into single unit.
- Required communication or interaction between the bots and others when needed.
- Capable to work independently, highly flexible and segregated as well.

Swarm intelligence mainly decreases the task load by dividing the computational section evenly and reducing the interactions reliance on the system. This swarm of bots is favourable in those areas or spaces where human intervention is inconvenient.

7 CPS-Complex Problems and Its Simple Solutions

Everything that exists in this world has its own pros and cons. Now, let us discuss something about the various complex challenges to CPS and their unique solutions (Sanislav & Miclea, 2012; Horvath & Gerritsen, 2012).

(i) *Accommodation*:

This challenge is mainly divided into two categories.

a. Making assets manageable.
b. Adjusting CPS in the environment.

An effective accommodation can be achieved by the following:

a. Selection of unchanged yet common and uniform data exchange that will benefit in: one is information retrieval and the second is connecting with universal data bus using the set of instruction and linking.
b. Transfer of current assets all in one go.

(ii) *Tradition*:

CPS generally faces this challenge where the roles of both human and machine together comes into play. An ideal illustration of this scenario is factories where machine and human labour is required to work simultaneously on the same platform. On a broader spectrum, it has been noticed that technology is leading to less of human requirement and thereby increasing the rate of unemployment day by day. Therefore, the technology makers must:

a. Take care of the human value in digital ecosystem, documenting the machines as a helping hand and not a threat to human survival.

b. Understand the variations in ecosystem and the digital culture and promote new innovations.
c. Approach a comprehensive way of defining this technology in order to embrace it and to make use of it as much as possible to its greatest value.

(iii) *Safety and Security*:

Safety and security are the most important, yet most complex issue. The interconnection between the processes and the machines often leads to various susceptibilities that later becomes a major threat to the system. Nowadays, along with the integration or merging of multiple technologies like IoT and CPS, there may be chances that a system may have to get attacked by certain worms or viruses that may lead to the destruction. Therefore, it automatically becomes necessary to look at the safety issues. Potential solutions to this challenge are as follows:

a. Constructing an interface in between that will secure the integration from various malware, viruses, worms, etc.
b. A new strategy must be established that will handle various unfortunate events and restricts the things that will lead to damage.
c. Proper monitoring and rules and regulation along with alerts that may prove to be beneficial in the digital world.
d. The system must be designed in such a way that it becomes independent and capable enough of solving the security issues on its own.

(iv) *Skill Requirement*:

With the rapid growth of this emerging technology (CPS), it will not only provide new opportunities, but may also terminate the human requirement completely. It may lead to various issues such as the increase in the human degradation and inequality which further leads to a lot of health issues and loss of lives. Therefore, in order to find a potential solution, following points need to be taken in consideration:

a. New methodologies need to be constructed that would require existing skill set as well as gaining new technologies that could be applied to this digital environment.
b. A proper balance needs to be maintained between the human and machines making it friendlier so that both can work in collaboration with each other. This will definitely overcome this challenge and will create harmony.

8 Applications of Convergence of CPS and Robotics

CPS has excelled in almost all fields that include self-propelling systems, agriculture, manufacturing industries, health care, defence, smart cities, traffic control and safety, power generation and distribution, smart grids (energy conservation), water management systems, transportation, security and robotics (Electronics Tutorial, Merriam-Webster; Pratt et al., 1999; De Roever et al., 1998). Some of them are listed as follows in Fig. 2:

(i) *Smart Cities*:

CPS plays an important role in building smart cities. Some of the advancement areas of CPS that are required for smart cities are as follows:

a. Smart industry
b. Smart health care
c. Smart energy
d. Smart infrastructure
e. Smart mobility

(ii) *Transportation*:

An ideal illustration is driverless cars, that is, its two-dimensional sensors, three-dimensional sensors, speed cameras, etc., which are highly used in scanning an ecosystem and a path for its movement and hence making a decision on its own with or without human intervention.

(iii) *Smart Grids*:

Smart grids are deliberately called as a CPS with some additional features of cyber-system and physical technique. This engages advanced observation, control and various interaction systems that yield a safe and secured energy supply.

(iv) *Emergency*:

There can be various emergency situations in which the robots can help humans in their survival for example, a case can be when the fire alarms go off in an indoor such as office, schools, hotels, hospitals a team of robots and supervisors can save the life of people. For this, initially a emergency alarm can be generated. Then the robots will start locating humans (using the face recognition or fire marshal dress

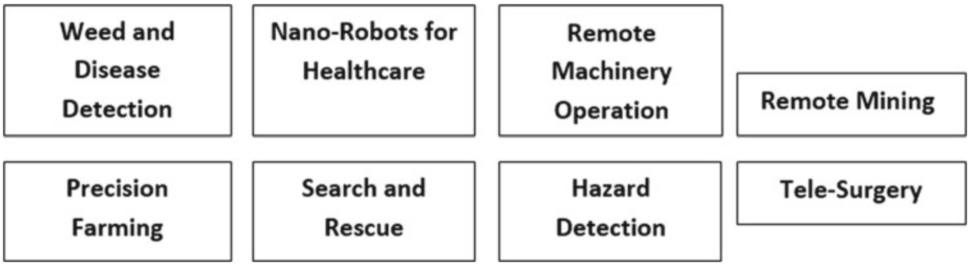


Fig. 2 Various applications of convergence of CPS and robotics

code). After this they try to find the possible exit path and try to eliminate the obstacles, and they can help humans to navigate from the hazardous situation. They mark the path to the exit with LED lights marked on the robots. If the victims are still inside in danger, then a message is sent to identify people at risk and mark out the supervisor. Send voice message after a fixed time if victims are still inside.

(v) *Microbots*:

The field of robotics has the capacity of varied medical tasks like endoscopy. With the release of microbots in the bloodstream, the anomalies can be detected. Other programs which they are capable of are sewing tissues can deliver the drug to the desired target, etc. The concept of remote surgery is also based on these robots. The world's first robotic heart surgery was performed from a remote location by a doctor with robotically controlled machines. Now with the emergence of CPS, the geographical boundaries will be demolished and every person will be provided with required treatment.

9 Collation of Cyber-Physical System and Internet of Things

Cyber-physical system is proving to be the smartest systems of the decade. They can turn to be an interface between various physical and logical components of a robot and are collaborating with robotics industry for successful and productive interaction of computational elements with that the amalgamation of algorithms.

Once the components of a robot are intact and interrelating properly, it is time to work on the various operations which a robot is expected to perform. The whole physical system which is embedded inside the robot is steered via data collection, observed analytics, smart optimization and networking. IoT interconnects people, systems and information leading to process and reacts physical and virtual world altogether (Manyika et al.).

If CPS is responsible for adaptability, surveillance, culture and skill development then IoT deals with real-world needs, opportunities and protocols. The partnership between CPS and IoT will boost the robotics industry, innovation, speed economy of the world. Their convergence will conduct the arrival of more complex, safe and secure robots. Industries and organizations will rely on these machines for agriculture, infrastructure, aeronautics, medicines, transportation, etc. Thus, IoT is the subset of CPS.

9.1 Alliance of IoT and CPS for Robotics

Till now we have seen how IoT is treated as a subset of CPS and what are the various features of CPS and IoT in terms of robotics. The process of convergence is described in Fig. 3. At Level 1 we have the robotics industry, creating a fusion of cyber-physical system and IoT together, which leads them to Level 2 which is the Internet of services. Internet of services contains everything which is required to use a software application; this includes software, its tools of development and the platforms through which it is connected to the Internet. Moving forward, there is a physical system that is efficiently interacting with the internal constituents of a robot like the data and algorithms that is why calling them a synergy means two components that are not that effective separately but can provide better output linked together. Lastly, the robot is ready for the human–robot interaction.

9.2 Constituent Classification

During the convergence of CPS and IoT in robotics, there can be various underlying constituents in the background. They can be classified as corporeal constituents, analytical constituents and transmission constituents (Acatech, 2011; PICASSO Opportunity Report; Stojmenovic & Zhang, 2015; Cyber-Physical Systems—Virtual Organizations).

(i) *Corporeal Constituents*: If we talk in respect of the Internet of things and cyber-physical system, then corporeal constituents are those constituents that are existent or virtual, mobile in time and space, and also are detectable.

In terms of the engineered systems of robots, it is specifically an assembly of various physical or instinctive components that are capable of performing various functions

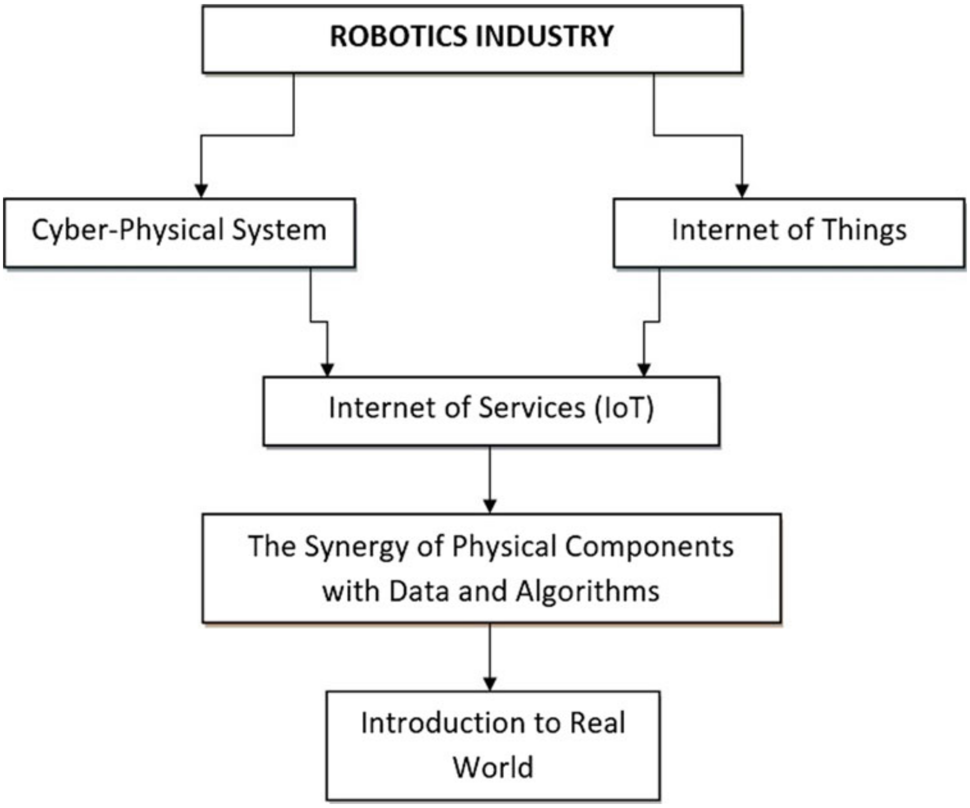


Fig. 3 Interactivity model

which includes constructional and practical requirements, e.g. energy alteration. Sometimes the corporeal environment with which the robot system interacts is also taken into consideration as an elementary interest. These constituents are termed as entity i.e. those real-world objects which are distinguishable from all the other real-world objects. Each entity in a robot system is separate and is user friendly, they can be any gadget or domain from sapiens to machinery, from electrical appliances to any computer.

In a robot system, there can be vigorous systems which include switches, motors, etc., and submissive systems which include structural elements, frames, etc. These systems are building blocks of a robot to interact with the physical surroundings, people and other factors.

(ii) *Analytical Constituent*: Another important aspect of any robot system is analytical constituent which includes facts, figures and conveying technologies. The major criterion of this particular section is that it helps in creation, manipulation, organization, analysis, managing and controlling of the unprocessed data for the robot system. The major advantage of it is that it is not bounded by any internal or external equipments, scanning, hardware, operating systems, computers, etc. It consists of three necessities the data, details and comprehension as shown in Fig. 4.

Fig. 4 Analytical constituent necessities

Necessities
Data
Details
Comprehension

The data is processed, accessed, edited, organized and manipulated using electronic medium of communication for low execution time and more accessibility. Data is responsible for representing possessions of the entities associated with a robot. Then comes the details which handle various queries related to the whole mechanism of a robot, and it can be some technical questions that can arise during the processing. Lastly, there are comprehension, the answers which are present inside details need to be conveyed which is basically done by comprehension. Comprehension can be linked with the knowledge that fetches and then forward the explanation of certain questions.

In analytical constituent, humans play a major role in designing, organizing, working for the security, maintenance of the system which will process these above-mentioned necessities. The system may consist of hardware, software, commercial and non-commercial information of the robot, confidential data, etc. Defects are common bugs in a system and to prevent them a systematic approach towards the creation of a robot is very necessary for which the components incorporated in the hardware layer, i.e. peripheral devices, buses, fibre, etc., in software layer, i.e. handlers, operating systems, applications, etc., protocols, wired or wireless medium, raw data and information related to a robotic system needs to be protected from deformities.

(iii) *Transmission Constituents*: These constituents of a robot system basically act as a connector between the corporeal and analytical constituents of a system. It includes transducers, sensors and actuators.

a. Transducers: Transducers focuses on providing a specific output of any particular input or in simple words, that is it converts energy from one form to another. The form can be mechanical, physical, chemical, etc., e.g. loudspeakers and thermometer.
b. Sensors: These devices are generally made work on the input of a system and they used to sense any change in the original behaviour of that input. The simplest example of a sensor is LDR, i.e. light-dependent resistors. It is seen that when light falls on a LDR the resistance becomes very less and vice versa when light is less.
c. Actuators: These devices are made work on the output of the system and are responsible for the movement and control of the system or in simple words the energy is converted into some sort of motion, e.g. switches, motor, etc.

There are three major subcategories in transmission constituents as shown in Fig. 5.

Firstly, we have to load which works as an input and it is majorly provided by the corporeal and analytical constituents of a robot system. Transform is used to work on this input and process it by including metadata, analysing, organizing, etc. Lastly, the product is achieved by the interaction of the input and the metadata. The input is converted with the help of transformation to provide a desired output of the robot system.

To make a successful robot, it is important to have all these three constituents in it because production of output is incomplete without input or its processing. Humans play a very emerging role in maintaining the process for gaining input to processing it and then finding the output from the same. All three processes include energy and then manipulating that energy for the transmission and converting it to some other form. A number of algorithms are possessed, managed and transformed which is handled by a whole team of researchers, developers, etc.

Ultimately CPS and IoT include these constituents while production of robots in which the physical components meet the internal components like data, information, algorithms, etc., needs to be managed properly by the humans to reduce the risk of malfunction and termination of a robot system.

Fig. 5 Subcategories in transmission constituents

Sub-Categories
Load
Transform
Product

9.3 Applications

With the enhancement of robotics industry with IoT and CPS, we now have various applications of robots that have increased the interest of people in this industry (IEEE; McClelland & Rumelhart, 1986; Anavangot et al., 2018; Singh et al., 2020a; Nayyar & Puri, 2016; Singh et al., 2020b; Dubey et al., 2020; Sehgal et al., 2020; Padikkapparambil et al., 2020; Singh et al., 2020c; Tanwar, 2020; Gupta et al., 2020). Some of them are:

(i) *Pepper*: Pepper is a human-shaped robot which is used in various stores of USA for interaction with the customers. It can understand their facial expressions and their tone in which they are speaking. It has made the billing system of the stores easier and faster.
(ii) *Sophia*: It is the first humanoid robot which is interviewed in various television shows talking about its efficiency and smartness. Sophia cracks jokes, makes facial expressions, she can dance and also have a good confidence. She is the first humanoid robot to get a full citizenship of the country. One of the best qualities of Sophia is that she can even sing and maintain eye contact with a person.
(iii) *Robotic Kitchen*: It is a robot which is embedded in a kitchen. It has hands, oven and also a screen in which the person can efficiently interact with the robot. This robot has a separate library in which there is a collection of recopies. This robot can cook something from that collection.
(iv) *Voice Assistants*: These are not actual robots but still they are widely used all over the world. They have people's work easier as they come with various features like reminders, calling facility, notifying about important things, etc.

These applications are a step towards greater economic, social and human growth.

9.4 Significance of Convergence of IoT and CPS in Robotics

Till now it has been seen that how two different terms IoT and CPS when merge together in robotics create unstoppable robots. We learned about the basic idea of the whole process which is involved in the journey of creating an interactive robot. This section of the chapter describes that what changes have come with this revolutionary convergence and how is it significant to humans (IEEE).

Both CPS and IoT have escalated accomplishment, versatility, extensibility, durability, welfare, certainty and convenience in today's world. Our future is going to fill up with humanoid robots which will help us in every sphere of life and to accomplish that the revolution has begun. Humans were born to adapt to changes and with such a change, everything will be going to be modified (McClelland & Rumelhart, 1986). Stationary machines will now be replaced with mobile robots, convergence of CPS and IoT in robotics will take over the advancement of the world.

By the shocking results and effective outputs of this convergence, the researchers, developers, industries, etc., are involving into it with more interests and passion. This convergence has proved to be a favour in many sectors like agriculture, IT sectors, businesses, research, etc. It has broadened opportunities for making engineering more interesting and complex.

9.5 Future of the Robotics

Robotics and automation will be having a profit amount never seen before. Smart data analytics will be having a positive impact on businesses and also the government (e-governance) will be benefited. We will be having the new platform across the world very soon. The goal is to minimize or even eliminate the needed of people's help for activities like growing crops, packaging, delivering goods to get benefit from the machines to adapt the changing conditions. Consumer robots are not yet a part of the current frame, but IoT could feed it with the higher rate of adoption. Statistics say the market worth of IoRT will reach $21.44 billion by 2022. An increase of 12% is predicted till 2022 in the robotics industry due to the presence of interconnectivity among IoT, CPS and robotics as shown in Fig. 6.

It is not impossible to imagine the market value of consumer robotics. Another way of combining IoT, CPS and robotics to help people can be seen through telepresence robots. They are operated from a remote location or from a distance through keyboard. The capabilities of robot's video and audio can help a person to have meeting or attend the classes in school without being physically present on the site.

Insects have been seen as small but they came up with very unique solutions for future robotic field. The design can be used to make spy robots, used in projects which require more features but have less space. Microbots are still in development which can flow into the bloodstream and treat the patient. This could be considered as a boon for healthcare department. The future is very bright for IoT, CPS and robotics and their collaboration is one of the fastest developing areas of technology. The future belongs to robots.

10 Conclusion

Robotics has already proven its capability and its development speed is also commendable, but the vision we have for the field of IoT, CPS and robotics is beyond what we are seeing today. The ultimate aim is to make machines which can gather data from the web and other devices and perform desired tasks, provided they should be cheap, efficient and time saving.

The IoT- and CPS-aided robots still have a long journey, but the rate of our progress on a daily basis ensures that baffling innovations are expected any time soon. The greatest union of IoT, CPS and robotics was ignored by IT specialists, but now they have also realized that the future depends on these applications which pair up to which autonomous machines to seamlessly reshape the robotics industry with the help of IoT and CPS.

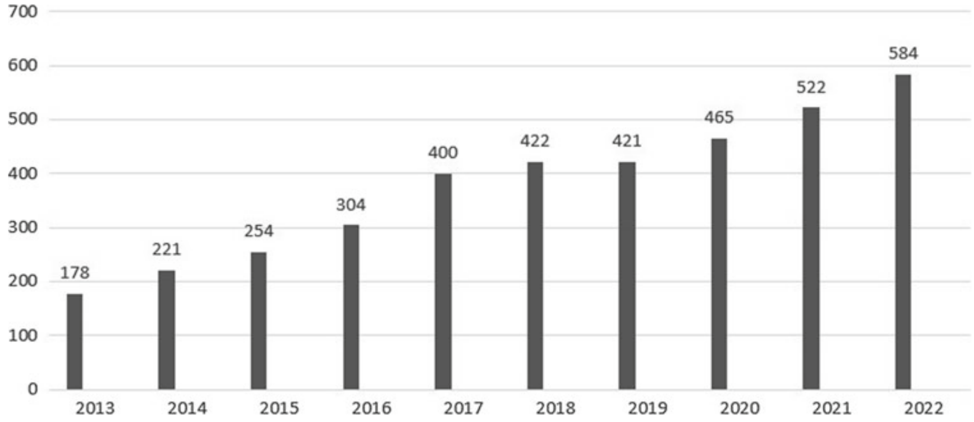


Fig. 6 Increasing rate of annual installations of industrial robots 2013–2018 and 2019–2022

The future of robots is hidden until we consider them as "things" which show compatibility witch the devices near them. By combining technologies, we will be able to produce solutions which are more capable than ever seen. This is possible by providing them with data. Perhaps the increased requirement of robots across the market place will expand the horizon of most IoT and CPS applications, which will enhance the autonomous machines sector.

In the end, we can just say that humans will be seeing an era which will make even complex problems easy to solve with efficiency and they will for sure we time saving and will be economically beneficial. We will be having technology as a solution to almost every problem.

References

Acatech. (2011). Cyber-physical systems driving force for innovation in mobility, health, energy and production. Position paper. Munich, Germany: National Academy of Science and Engineering.

Anavangot, V., Menon, V. G., & Nayyar, A. (2018). Distributed big data analytics in the Internet of signals. In *International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 73–77).

Ashton, K. (2009). That 'Internet of Things' thing. *RFID Journal*.

Atzori, L., Lera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54,* 2787–2805.

Batth, R. S., Nayyar, A., & Nagpal, A. (2018). Internet of robotic things: Driving intelligent robotics of future-concept, architecture, applications and technologies. In *4th International Conference on Computing Sciences (ICCS)* (pp. 151–160).

Cyber-Physical Systems—Virtual Organizations. Internet of things & cyber-physical systems. https://cps-vo.org/group/iot.

De Roever, W., Langmaack, H., & Pnueli, A. (1998). Compositionality: The significant difference. Papers from the International Symposium on Compositionality COMPOS'97. Berlin, Heidelber: Springer.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Electronics Tutorial. Sensors and transducers. https://www.electronicstutorials.ws/io/io_1.html.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Horvath, I., & Gerritsen, B. (2012). Cyber-physical systems: Concepts, technologies and implementation principles. In *Proceedings of the Tools and Methods of Competitive Engineering* (pp. 7–11). Karlsruhe, Germany: Delft University of Technology.

Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., & Astorga-Vargas, M. (2017). Tracking the evolution of the internet of things concept across different application domains. *Sensors, 17* (6), 1379, 1–24.

IEEE. IEEE Standard Computer Dictionary: A compilation of IEEE standard computer glossaries. https://ieeexplore.ieee.org/document/182763.

IEEE Technical Committee on Cyber-Physical Systems. https://www.ieeesystemscouncil.org/pages/cyber-physical-systemstechnical-committee.

Kim, K. D., & Kumar, P. R. (2012). Cyber-physical systems: A perspective at the centennial. In *Proceedings of the IEEE 100 (Special Centennial Issue)* (Vol. 100, pp. 1287–1308). IEEE Press.

Koreshoff, T., Robertson, T., & Leong, T. (2013). Internet of Things: a review of literature and products. In *OzCHI '13 Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (pp. 335–344). Adelaide, Australia: ACM.

Lee, E. (2006). Cyber-physical systems—Are computing foundations adequate? Position paper. In *NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, Austin, TX.

Lee, E. (2010). CPS foundations. In *DAC '10 Proceedings of the 47th Design Automation Conference* (pp. 737–742). Anaheim, CA: ACM.

Li, S., Xu, L., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers, 17,* 243–259.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. The internet of things: Mapping the value beyond the hype. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx.

McClelland, D., & Rumelhart, J. (1986). *Parallel distributed processing* (12th ed.). Cambridge, MA: The MIT Press, A Bradford Book.

Merriam-Webster. Actuator. https://www.merriamwebster.com/dictionary/actuator.

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet of Things*, 1–86.

National Institute of Standards and Technology. (2013). Foundations for Innovation in Cyber Physical Systems Workshop Summary Report. Prepared by Energetics Incorporated Columbia, MD.

National Research Council. (1995). *Expanding the vision of sensor materials*. Washington, DC: National Academy Press.

National Science Foundation. Cyber-physical systems (CPS). https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.

Nayyar, A., & Puri, V. (2016). A review of Arduino board's, Lilypad's & Arduino shields. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1485–1492).

Nayyar, A., Puri, V., & Le, D. N. (2017). Internet of nano things (IoNT): Next evolutionary step in nanotechnology. *Nanoscience and Nanotechnology, 7*(1), 4–8.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 217–243).

Pallás-Areny, R., & Webster, J. (2001). *Sensors and signal conditioning* (2nd ed.). New York, NY: Wiley.

PICASSO Opportunity Report. Towards enhanced EU-US ICT pre-competitive collaboration (European Union's Horizon 2020 Research and Innovation Programme funded PICASSO). http://www.picasso-project.eu/wp-content/uploads/2017/03/PICASSO-OpportunityReport_March-2017_revMar19.pdf.

Pratt, D., Ragusa, L., & Von der, L. (1999) Composability as an architecture driver. In *Proceedings of the 1999 Interservice/Industry Training, Simulation and Education Conference* (p. 96). Orlando, FL: National Training Systems Association.

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. In *Proceedings of the 47th Design Automation Conference* (pp. 731–736). Anaheim, CA: IEE.

Sanislav, T., & Miclea, L. (2012). Cyber-physical systems—Concept, challenges and research areas. *Journal of Control Engineering and Applied Informatics, 14*(2), 28–33.

Sarma, S., Brock, D. L., & Ashton, K. (2000). *White paper: The networked physical world: Proposals for engineering the next generation of computing, commerce & automatic-identification*. Cambridge, MA: MIT Auto-ID Center.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Shi, J., Wan, J., Yan, H., & Suo, H. (2011). Survey of cyber-physical systems. In *Proceedings of 2011 International Conference on Wireless Communications and Signal Processing*. Nanjing, China: IEEE.

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020a). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet, 12*(4), 61.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020b). *Internet of Things: From hype to reality. An industrial IoT approach for pharmaceutical industry growth* (Vol. 2, p. 191).

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020c). Internet of Things in pharma industry: Possibilities and challenges. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 195–216).

Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In *Handbook of research on big data and the IoT* (pp. 379–405). IGI Global.

Stojmenovic, I., & Zhang, F. (2015). Forward: Inaugural issue of 'cyber-physical systems'. *Cyber Physical Systems, 1*(1), 1–4.

Tanwar, S. (2020). Fog data analytics for IoT applications—Next generation process model with state of the art technologies. *Studies in big data* (Vol. 76, pp. 1–497). Springer.

Whitmore, A., Agarwal, A., & Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274.

Woodside, A., & Sood, S. (2016). Vignettes in the two-step arrival of the internet of things and its reshaping of marketing management's service-dominant logic. *Journal of Marketing Management, 33*(1–2), 98–110.

IoT, IIoT, and Cyber-Physical Systems Integration

Halim Khujamatov, Ernazar Reypnazarov, Doston Khasanov, and Nurshod Akhmedov

Abstract

In recent years, new concepts as IoT, industrial IoT, and cyber-physical systems have emerged with the active penetration of information and communication technologies into industrial processes. Interrelationships between these conceptions and the degree of integration between them are considered the apotheosis of modern days. As a result, this chapter focuses on the integration of IoT, industrial IoT, and cyber-physical systems. It provides analytical data on the industrial revolution and Industry 4.0, information about IoT, IIoT, and cyber-physical systems for smart environments, their history, development trends, definitions, architectures, components, applications, and characteristics. Also, IoT, IIoT, and cyber-physical systems were compared in terms of origin, application, architecture, characteristics, and the degree of integration between them was determined. Studied following issues of integrated IoT, IIoT, and cyber-physical systems—control issues, network construction issues, computing issues, and security issues.

Keywords

IoT • Industrial IoT • Cyber-physical systems • Integration • Smart environments • Applications • Architecture • Control • Networking • Computing • Security

1 Introduction

From a multitude of technologies and their interconnections, the industrial Internet of things has evolved. The first attempts to build a web of “things” in manufacturing date back to the 1970s and were summed up by the term computer-integrated manufacturing (CIM) in the 1970s. While the concepts behind CIM are now nearly 40 years old, most of the challenges are still relevant today, such as integrating management and engineering processes and implementing flexible and highly automated automation.

In the 1990s, however, with the growing popularity of the phenomenon of lean manufacturing, over-IT strategies were gradually deemed ineffective, and many CIM projects failed. In retrospect, early frustrations may stem from the fact that technology and people were not prepared to execute ideas successfully. The factors that did not allow the implementation of CIM ideas include the following points:

- Insufficient IT and communication infrastructure;
- Insufficient computing power;
- Insufficient data storage capacity;
- Lack of openness of data sharing software tools and formats;
- Limited connectivity and rates of data transfer.

While CIM focused on shop floor solutions, product data management (PDM) was developed as a new approach to designing networks within engineering departments linking product and human resources data. In contrast to CIM, PDM technologies seemed less technologically disruptive, but their emergence was made possible by reaching the limits of processing large amounts of product data using simple file systems. Features such as product configuration, workflows, updates, or authorization are now necessary for large enterprise engineering departments and are becoming increasingly relevant for mid-sized businesses. The idea of a network is exploding with product lifecycle management

---

H. Khujamatov · E. Reypnazarov (✉) · D. Khasanov · N. Akhmedov
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
e-mail: reypnazar0vernazar@gmail.com

H. Khujamatov
e-mail: kh.khujamatov@gmail.com

D. Khasanov
e-mail: dhasanov0992@gmail.com

N. Akhmedov
e-mail: axmedov.n.m@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_3

(PLM) technologies, with transparent data management as a target for the entire life cycle. In this sense, PDM is commonly seen as the core of PLM, offering interfaces over the entire life cycle for different applications, such as manufacturing and services. As a result, PDM and PLM are also a prerequisite for IIoT: as a basis for practical communication, industrial "stuff" requires product data, for example, to equate calculated data with originally defined product-related criteria.

While PLM and the digital factory are undoubtedly contributing to the development of IIoT, many of the ideas for IIoT hardware design come from cyber-physical systems (CPS) and mechatronics. In general, mechatronics is characterized as a discipline combining mechanics, electronics, and information technology. The discipline can be seen as an extension of mechanics, as the word "mechatronics" in the first syllable indicates, and many stakeholders have mechanical engineering experience. At the same time, the name "cyber-physical system" was introduced into everyday life by researchers from the field of computer science and software. For example, NASA defines CPS as "an emerging class of physical systems that can exhibit complex behaviors through embedded software." A similar definition is used in the CyPhERS project roadmap: "CPS consists of computing, communication and control components in combination with physical processes of a different nature, such as mechanical, electrical and chemical." The latter definition can also apply to mechatronic systems, and the words mechatronics and CPS are often used interchangeably, especially in the automation and transport sectors. Nonetheless, from a traditional point of view, "mechatronics" implies that the focus is on the physical system with advanced software development, while the definition of cyber-physical systems rather indicates that most of it is software-based and that the hardware is a particular problem for development software because of the spatiotemporal interaction with the physical environment. In addition, communication between subsystems that are not inherently part of mechatronics characterizes CPS.

CPS can be defined as a networked system in this context, and the sense of network is typically implicitly included in the term CPS, for example by type definition: CPS includes "embedded computers and networks that monitor and control physical processes." Continuing with the idea of a network, CPS can be seen as an "IoT support vehicle," IoT means that the subsystems are connected to the Internet and are thus part of an open system with a large number of nodes.

Presently, most researchers agree that CPS and IIoT are moving forward for applications like Industry 4.0 and will have a large economic impact. To be sure, the transition to Industry 4.0 is not an end in itself, but it can lead to greater resource productivity, shorter time to market, lower final product prices, and the introduction of new services. Specifically, implementations and prospective advantages involve:

- Smart automation, allowing to reduce the serial production, as reprogramming and commissioning are carried out in real time;
- High resolution manufacturing that increases predictability and cost transparency;
- Smart production planning, which increases delivery time enforcement and decreases costs and lead times;
- Predictable automatic fault detection and maintenance, resulting in increased overall equipment efficiency and lower costs of maintenance;
- Intelligent management of processes aimed at zero waste, low cost of instruments, reduced use of energy and short run-in and output times;
- Reconfigurability, providing fast scaling and management of changes in the production process;
- Contact between humans and computers leading to increased efficiency and better ergonomics;
- Input from production to engineering that enhances manufacturing systems of the next generation;
- Implementation of new business models.

While CPS and IIoT tend to have a wide range of approaches, applications from other areas such as energy, transportation, or health care cannot be directly involved. Features of IIoT and CPS include:

- Factory integration of machines and their components;
- Heterogeneous infrastructure for production from various suppliers;
- Alignment of the product life cycle and of production resources;
- Spatiotemporal relationships in the system between objects;
- Introduction of new technologies into technologies with equipment already in operation;
- A wide range of technologies for production.

Typically, both IIoT and CPS can be viewed as complex system. Consequently, there are several technological foundations for creating such systems, which leads to the first major challenge: choosing a suitable technological framework and architecture. The specification of commonly agreed, extensible infrastructures or an architectural pattern that, on the one hand, must accommodate different sensors, actuators, and other hardware and software systems is another major challenge, although, on the other hand, the device must remain manageable. Not only sensor equipment, but also control or planning systems that provide access to organizational information should be in place for such a networked system. Researchers as well as industrialists have implemented many pseudo-standardized architectural solutions in order to handle diverse structures and ensure that knowledge needs are met. For example, the automation pyramid or the more advanced automation Diabolo, representing such architectural solutions, is well recognized in the field of automation. With the introduction into the automation industry of CPS and IIoT, these job-specific and well-structured templates are helping to quickly resolve manufacturing problems.

Based on the above, the study of the interrelationships of new concepts such as IoT, IIoT, and CPS and the degree of integration between them is a topical issue today. This chapter intends to explore the meanings of the concepts of IoT, IIoT, and CPS and the relationships between them.

The chapter consists of ten paragraphs, the first of which gives a short overview of Industry 4.0 and the principles of its implementation.

The second paragraph provides information on IoT for smart environments, its history, development trends, definitions, architectures, components, applications, and characteristics.

The third paragraph provides information on IIoT for smart environments, its history, development trends, definitions, architectures, components, applications, and characteristics.

The fourth paragraph provides information on CPS for smart environment, its history, development trends, definitions, architectures, components, applications, and characteristics.

In the fifth paragraph, the concepts of IoT, IIoT, and CPS are compared from different perspectives. Their comparison is based on differences in origin, application, architecture, and characteristics.

The sixth paragraph identifies the degree of integration between the concepts of IoT, IIoT, and CPS.

The seventh paragraph deals with the management system in integrated IoT, IIoT, and CPS systems, i.e., the principles of centralized, decentralized, and hierarchical management, the eighth paragraph about network technologies used in their implementation, the ninth paragraph about the computing system, and the last tenth about security issues.

2 Industry 4.0

The concept of digitalization, which has grown strongly in recent years, is the foundation of industrial revolution 4.0., i.e., the mass implementing of CPS in other areas of human life such as production and domestic life, work, leisure. The term Industry 4.0 was one of the 10 drafts of Germany's state strategy for technological development until 2020 in 2011. In general, Industry 4.0 encompasses definition of smart industry based on global industrial network services and IoT, including changes in normal life, work, and leisure life (Minerva et al. 2015).

Industry 4.0 aims to integrate data, tools, and processes from a variety of applications to reduce overall costs, reduce risks, and increase efficiency through the use of CPS. At the same time, unlike previous industrial revolutions, it is not based on a single technology, but on the following basic technologies (Anavangot et al. 2018; Kumar and Nayyar 2020; Tanwar 2020):

- *Big Data.* Big data is a description of organized and unstructured data of immense quantities and considerable diversity, easily handled in the late 2000s by horizontally distributed computing technologies and an alternative to conventional business intelligence class database management systems and solutions;
- *Internet of Things, IoT.* The Internet of things (IoT) is a definition of a virtual network of physical objects fitted with built-in technology to communicate with each other or with the external world, considering the organization of such networks as a phenomenon capable of restoring economic and social systems, excluding from the part of behavior and operations the need for human participation;
- *Cloud Computing.* Cloud computing is a model for offering convenient on-demand network access to any traditional pool of configurable computing resources that can be easily provided and released to the provider with minimum running costs or calls;
- *Methods and tools of Artificial Intelligence, including Machine Learning.* Artificial intelligence (AI)-the property of smart devices to execute imaginative tasks that are historically considered a person's prerogative; science and technology to build smart machines, in particular smart computer programs. Machine learning (ML) is a class of techniques of artificial intelligence, a distinguishing characteristic of which is not a straightforward solution to a problem, but learning through the course of applying solutions to several related problems. Mathematical statistics instruments, computational approaches, optimization methods, probability theory, graph theory, diverse techniques for dealing with data in digital form are used to construct those methods;
- *Virtual and augmented reality.* Virtual reality (VR) is a world created through technical means that, by its senses, is conveyed to an individual: touch, hearing, sight, and others. Digital reality simulates exposure as well as exposure reactions. Software synthesis of augmented reality properties and responses is done in real time to construct a persuasive complex of sensations of reality. Augmented reality (AR) is the product of the incorporation into the area of interpretation of some sensory

evidence in order to complement ambient knowledge and enhance knowledge interpretation;

- *3D printing.* A 3D printer is a numerically operated device that utilizes a component's layer-by-layer printing process. 3D printing is a method of additive manufacturing which typically refers to technology for rapid prototyping. 3D printing can be achieved in different forms and with different materials, but either of them is based on the concept of the formation of a solid object layer by layer;
- *Printed electronics.* Printing electronics is an area of electronics that creates electronic circuits using printing equipment that allows you to apply special ink to the surface of a flat substrate and, thus, form passive and active elements on it, and see also inter-element connections according to the wiring diagram;
- *Quantum computing.* A quantum machine is a computational system used to move and process data utilizing the phenomena of quantum mechanics. A quantum computer (as opposed to a conventional computer) operates not with bits (capable of taking the value either 0 or 1), but with qubits that have values of both 0 and 1. Theoretically, this allows you to process all possible states simultaneously, achieving significant superiority over conventional computers in a number of algorithms;
- *Blockchain.* Blockchain is a continuous block sequential chain, which is constructed according to some rules and contains knowledge. The connection between blocks is provided not only by numbering, but also by the fact that each block contains its own hash-sum and hash-sum of the previous block. To change the information in a block, you will have to edit all subsequent blocks. Copies of blockchains are most commonly kept independently of each other on several different devices. This makes it extremely difficult to change the information already included in the blocks.

The use of IoT-based CPS in Industry 4.0 gave rise to the concept of industrial IoT. The following sections focus on these concepts, their similarities, and differences.

3 IoT for Smart Environments: Definitions, History, Architecture, and Applications

The word Internet of things was coined by University of Massachusetts researchers in 1999. There are several definitions of this term, which we consider to be relatively accurate:

The IoT is a network of physical objects based on internal technologies that allow us to interact with the external environment, transmit information about their status, and receive information from the outside.

Industrial IoT is an important part of the IoT. And a new term has already emerged, the Internet of everything, that is expected to replace the Internet of things in the near future.

The modern Internet consists of thousands of corporate, scientific, government, and home computer networks. The integration of networks in different architectures and topologies is done using the IP protocol. One permanent (static) or temporary (dynamic) IP address is assigned to each member (or group of members) of the network.

Similarly, today IoT consists of closely interconnected networks, each of which performs its own function. For example, in an office or apartment, it is possible to install several networks at the same time to control air conditioning, heating, lighting, security, etc. These networks can operate according to different standards, and combining them into a single network is a very important task. In addition, the fourth version of the IP protocol (IPv4) only allows access to 4.22 billion addresses, so there is a problem updating them. Even if every device connected to the network does not need a unique IP address (but still needs a unique identifier), the problem of lack of addresses can become a limiting factor due to the rapid growth of IoT. The sixth version of the IP protocol (IPv6) has helped solve this problem radically, giving every population of the Earth access to more than 300 million IP addresses (Krishnamurthi et al. 2019).

The main features of IoT architecture are: functionality, scalability, usability, and stability. We analyzed (Minerva et al. 2015; Wu et al. 2020; Hossein Motlagh et al. 2020; Ahanger and Aljumah 2019) and the three-layer, four-layer, and five-layer IoT architectures presented in them, and decided to provide the following three-layered architecture for IoT (Fig. 1):

Layer 1: Sensors and actuators;
Layer 2: Internet gateways and data collection systems;
Layer 3: Data center and cloud.

Let's take a look at each of the above architectural concepts:

First layer. Connected devices (sensors/actuators). The good thing about sensors is that it can turn the perceived information into a dataset that it can process for later analysis. They will make automated decisions and take action based on the collected information. For example: when someone enters a room, turning on a light or controlling doors and temperature, and so on.

Additional hardware can be used in this layer to obtain the information needed for further analysis.

Second layer. Internet or connection layer. In this layer, we understand that IoT works with nearby sensors and actuators. Internet access and data acquisition systems (DAS) play an important role here. DAS units are connected to the network of sensors. At the other hand, the Internet gateways operate with Wi-Fi, wired LANs, and perform further processing.

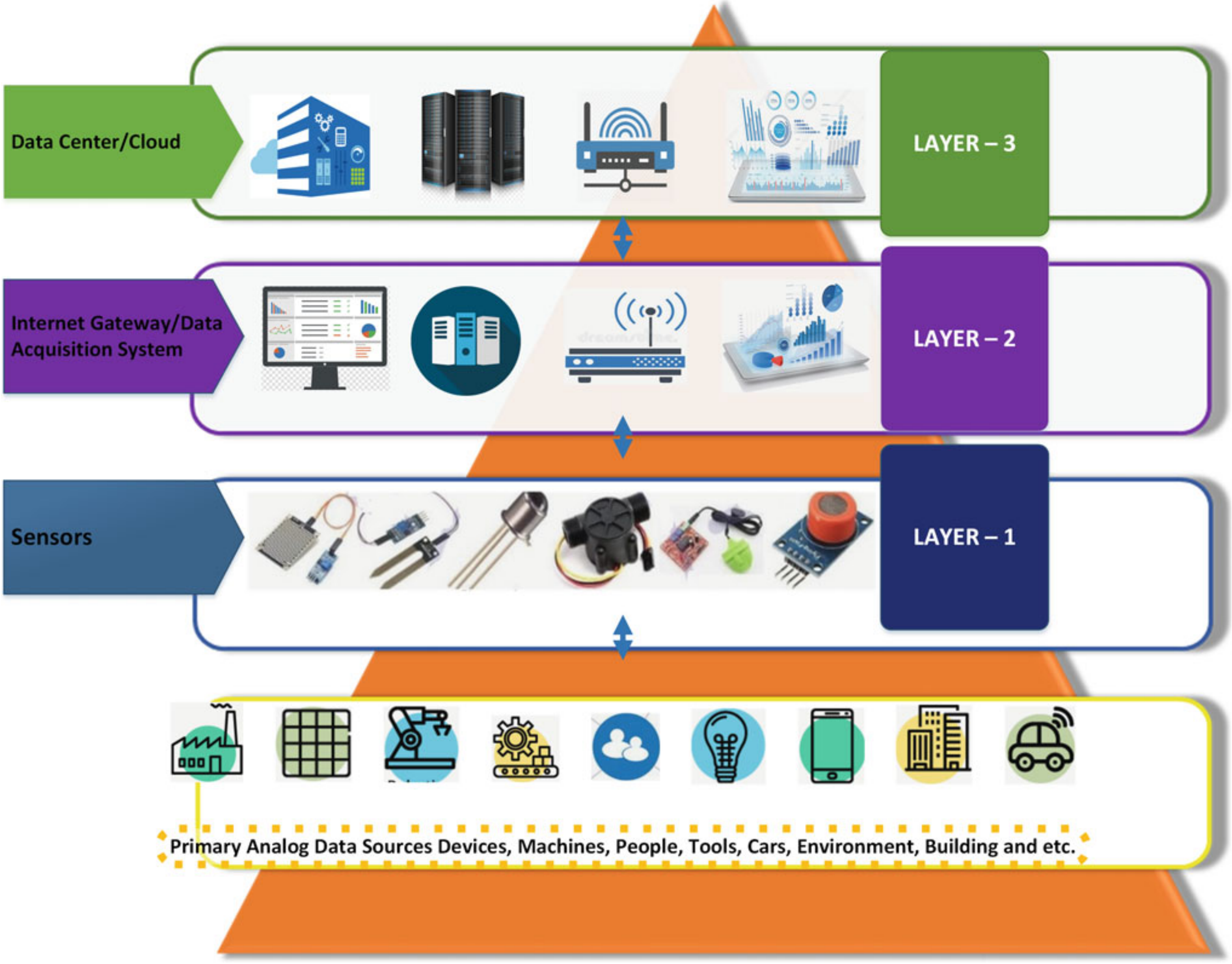


Fig. 1 IoT architecture

This layer is critical for processing and compressing the data collected in the previous layer for further analysis to the optimum size. On top of that, changing the time and changing the structure is done at this stage.

In short, Layer 2 helps to collect and digitize data.

Third layer. Data analysis, visualization, and storage. Here, in the final stage, the data in the data centers is deeply processed. This layer requires highly qualified applications as well as qualified IT professionals. Data can also be collected from other sources for execution. Once all quality standards and requirements are met, the data is returned to the physical world for predictive analysis.

It is also possible to include human intervention as an additional layer for the IoT architecture. It assumes that the existing process is user-controlled. The process may not require full automation (Solanki and Nayyar 2019; Batth et al. 2018).

Today, IoT is used in various fields. First, it is used in industry (IIoT), transportation, smart housing, utilities, health care, and agriculture. IoT is also used in trade, logistics, catering, hotel business, banking, construction and armed forces, and other fields.

In the long run, not only homes, but cities and even some countries will become "smart." However, at the current stage of technology and society development, IoT is being actively introduced not globally, but within companies producing goods, energy, transportation, etc., where efficiency and competitiveness are expected to increase due to new technologies.

4 IIoT for Smart Environments: Definitions, History, Architecture, and Applications

IIoT is the key component of the Industry 4.0 revolution. Industrial IoT is a tool for the implementation of Industry 4.0, providing full machine-machine communication (M2M), as well as software, computer networks, data collection with automatic remote control and management capabilities of production facilities and is a system that combines a single cycle with built-in sensors for sharing.

IIoT is almost identical to IoT architecture in terms of architecture as a specialized and more industrial-oriented version of IoT (Fig. 1). IIoT is based on the following hardware (Padikkapparambil et al. 2020; Singh et al. 2020):

- Identification tools. Every object in the physical world involved in IIoT must have a unique identifier, even if it is not connected to the Internet. Various available systems can be used to automatically identify objects: radio frequency, optical (barcodes, Data Matrix, QR codes), infrared metrics, and more. However, different types of identifiers need to be standardized to ensure their uniqueness.
- Measuring instruments. The function of the measuring instruments is to ensure that the information about the external environment is converted into appropriate information for transmission to the processing facilities. These can be temperature sensors, light sensors, and individual sensors or other complex measurement complexes.
- Data transferring tools. Any available technology can be used to transmit data. Particular attention is paid to improving the reliability of data transmission when using wireless networks. When using wired networks, an attempt is made to actively use data transmission technology over power lines, as many “items” will be connected to the power grid.
- Data processing tools. Due to the rapidly increasing number of digital data worldwide today, the main component of IoT is not sensors and data transmission tools, but cloud systems that provide high bandwidth and are able to respond quickly to certain situations. It also should be mentioned that edge and fog computing, which do not compete with cloud computing, but are capable of processing huge data streams that effectively complement them.
- Activators. These are devices capable of converting incoming digital electrical signals from information networks. For example, to turn on a home heating system with a smartphone, it must have a compatible device. Activators are often systematically integrated with sensors.

In the first phase of IIoT implementation, controllers, human-machine interfaces, sensors, and actuators will be mounted in industrial equipment. As a result, it will be possible to collect information that will allow the administrator to obtain direct and systematic information about the state of production. The processed data is provided to all departments of the company. It helps to build relationships and make informed decisions between employees from different departments.

The data obtained can be used to avoid unscheduled failures, equipment delays, unplanned repairs and failures in supply chain management, thereby allowing the company to function more effectively.

When a large amount of unstructured data is processed from sensors, filtering and adequately interpreting them becomes a priority. Therefore, it is important to present the information in a way that is understandable to the user. To do this, we use analytical platforms designed to collect, store, and analyze information about real-time technological processes and actions (Minerva et al. 2015).

IIoT allows you to create economical, flexible, and more efficient manufacturing. It is used actively in the manufacture of wireless devices, including smartphones, tablets, and sensors, that support IP. The current wired sensor network will be extended and complemented by wireless networks in the coming years, which will greatly increase the usage of tracking and control systems in industries. A progressively dense integration of the best information and operational technology characterizes the next step of optimization of production processes (Minerva et al. 2015).

IIoT solutions can increase manufacturing efficiency several times, and the payback period of IIoT projects often does not exceed a few months.

The main technologies and trends in the development of IIoT are (Dubey et al. 2020):

- The main components of IIoT are advanced analytical tools, artificial intelligence, and machine learning. This allows for active operational management and decision making of production based on in-depth analytical analysis.
- IIoT adds edge computing capabilities. This leads to data analysis closer to the data sources, increased information security, and improved production and product quality.
- The emergence of digital copies. With the introduction of IIoT technologies, digital copies of physical objects are emerging. These copies allow you to model, test, and optimize this object in a virtual environment before using it in a real environment.
- Auxiliary and virtual reality (AR/VR) technologies contribute to the development of IIoT. New staff trained on the basis of AR/VR technologies can mimic the real situation in the enterprise, the functions, management, and physical objects of employees with a high degree of confidence.
- Message Queue Telemetry Transport (MQTT) as the main protocol of message exchange in IIoT. MQTT is a simplified communication protocol based on TCP/IP. It is well suited for use in controllers and sensors that require

small codes and have channel bandwidth limitations. Therefore, MQTT is the main protocol of IIoT.

5 CPS for Smart Environments: Definitions, History, Architecture, and Applications

Ellen Gill from the USA first coined the term "Cyber-Physical System" (CPS) to describe distributed systems in which data processing is performed independently of its physical elements.

Systematic analysis of CPS technologies allows us to highlight the following areas of knowledge that are closest to it: real-time embedded systems, automated control systems of technical processes and facilities, distributed computing systems, IoT, industrial IoT, wireless sensor networks, machine to machine (M2M), fog computing, edge computing and cloud computing, complex adaptive systems, agent-based industrial systems. Many researchers argue that the concept of a CPS originated in the space of real-time systems. Naturally, the next step in the evolution of such systems was to connect different devices into a single computer network and ensure their interconnection via Internet protocols (IoT). The growing interdependence of computing and physical elements has necessitated a new interdisciplinary approach.

The essence of cyber-physical systems is that they combine physical production processes or other processes (e.g., power transmission and distribution management) and require real-time continuous control with practical software-electronic systems. It is also a new interpretation of the definition of embedded systems. At a new stage of development, the consideration of embedded systems as separate components that solve specific problems allows us to describe them as the basis of the whole process. One of the main challenges in this process is to synchronize a large number of different electronic devices over time in order to achieve cost-effective results. This challenge is important not only for manufacturing, but also for managing many systems that operate as part of smart city, such as energy water supply, smart transportation systems, smart homes, and more. It should be noted that the requirements for the synchronous operation of CPSs apply to the entire system, which determines the requirements for communication systems (wireless sensor networks, wired networks, and mixed data transmission systems) (Lee and Seshia 2016; Park et al. 2012; Siddikov et al. 2016, 2017).

Naturally, messages from millions of devices must be collected in processing centers, sorted by importance, priority, and other indicators, in order to automatically respond to a specific message or group of messages. Often, more information is required to optimize the economic and technical performance of a system. Big data solutions come here naturally, because of the large amount of data that can be processed. The requirements for the system, as well as for all components of the system are the same—synchronous operation in real time. It is the CPS that has led to the rapid growth of interest in real-time processing big quantities of data. It is one of the clear trends in the big data field (Namiot 2015). It should be noted that synchronization and real-time operation is not a very important factor for all digital economy systems. Some applications, such as digital medical applications, require a separate approach to the implementation of big data.

Features of the IoT architecture are also relevant to CPS architecture. So far, several types of architectures with different number of layers have been proposed for CPSs, depending on the system characteristics and different approaches. Based on these and an in-depth analysis of (Park et al. 2012; Liu and Jiang 2016; Sanislav 2017; Ahmadi et al. 2018), we decided to provide the following three-layer architecture for CPS (Fig. 2):

Layer 1: Connection layer;
Layer 2: Middleware layer;
Layer 3: Computing layer.

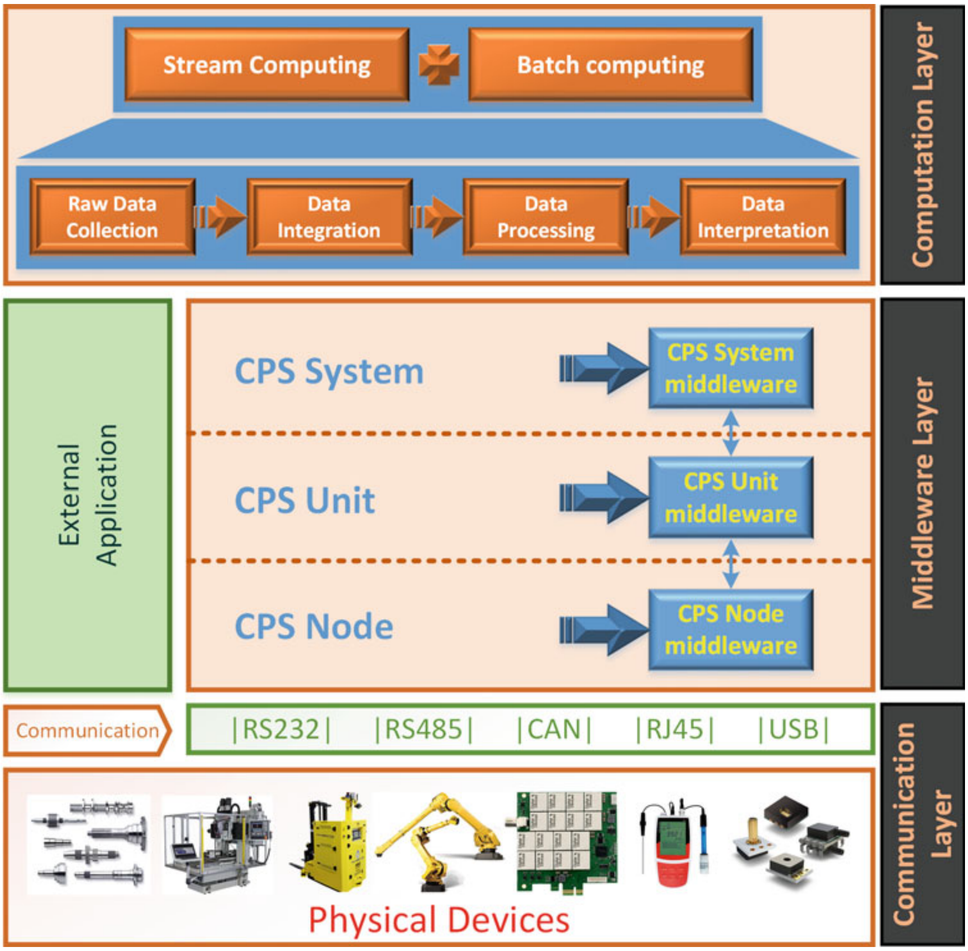
We will now describe each layer according to this architecture:

First layer. Layer of physical connections. Sensors perform one of the main functions in this layer. Various signals such as vibration, sound, temperature can be obtained by installing the correct sensor. The first phase in introducing CPS in industry and manufacturing is therefore to mount and distribute parts such as RFID devices, sensors, and measuring devices into manufacturing sources. Then, through industrial Ethernet technology or other technologies, a group of machines are connected. Protocol, location, distance, processing, and storage issues should be taken into consideration when selecting installed parts in this layer.

Second layer. Middleware layer. That layer transfers data gathered from installed parts for analysis to main server and sends it to the controllers to monitor the production commands (e.g., status monitoring, quality control, etc.) issued by the computing layer or external applications. The middleware layer in CPS thus acts as a link between the physical layer, the computing layer, and the application programs. The buffer will perform the following tasks, in conjunction with the above descriptions: system management, interface identification, and data management.

Third layer. Computing layer. In real time, various sensors, RFIDs, and measuring tools capture vast volumes of data online or offline. This is especially important when

Fig. 2 CPS architecture



machines operate under complex manufacturing conditions and experience a different type of disruption when dispatching rules are combined with data obtained through online data processing, measurement or data aggregation (Gupta et al. 2020). The two forms of big data computing which need to be considered in this layer are computing and streaming computing in one way. One-time computing is used for processing large quantities of stored data, and flow computing is used to process the flow of sensor data. The results are returned to the machine site for operation and process management and maintenance following a one-time calculation or flow computing. Thus, computing layer carries out the function of controlling machines or the self-production process. For example, this layer is responsible for integrating the knowledge produced with the experiences of people, thus providing a holistic view of the information, data, and knowledge for conscious decision taking.

CPS is smarter by applying information development and training methods in handling the manufacturing cycle, resulting in more output activities.

6 Comparison of IoT, IIoT, and CPS

As mentioned above, IoT, IIoT, and CPS are very closely related concepts. These terms have different origins and similar definitions, and are based on the trend toward integration of digital functionality into physical systems and devices, including communication networks and computing power. A detailed analysis of publications on relevant topics of the last decade shows that there is no general consensus among experts on the degree of interdependence of these terms.

To understand how the different definitions of IoT, IIoT, and CPS relate to each other, we consider objects at the component level that work with them. They include the following four categories of smart objects, which are determined by their functional capabilities (Ibarra-Esquer et al. 2017):

- Control objects: single-value identifiable mobile objects that are able to provide information about their current location;

- Data objects: objects that generate data by processing the signals of various sensors or based on their characteristics and current status;
- Interactive objects: objects that can interact with the environment in which they are located, measure various parameters of the environment and/or change them;
- Smart objects: objects that process information in some way and react based on the information obtained as a result of processing the relevant data.

If initially IoT technologies focused on control objects, now the concept has expanded to include (Khasanov and Reypnazarov 2019): objects equipped with different sensor devices (data objects), e.g., home facilities generating new data for analysis and creating additional personalized features and services; objects in active contact with material realm via remote-controlled transducers (interactive objects); as well as objects with analytical capabilities for flexible and sensitive interaction, such as autonomous vehicles (smart objects).

Initially, several IoT systems are system-of-systems where the components are a combination of data objects, control objects, interactive objects, or smart objects in themselves. Managing project specifications and assessing the quality of service (QoS) for each of these components is only possible in terms of the overall functional purpose and the interaction requirements with other components of the system (Ahmadi et al. 2018). The inclusion of the interaction of logical and physical components in the IoT concept brings it closer to the CPS concept, which is the result of the shift of developers' attention from control objects and data objects to interactive and smart objects. Indeed, many IoT solutions cited as examples of control objects or data objects, if we look at them from a functional point of view, it would be appropriate to consider them as components of an interactive or smart system. A single system or device can fall further into than one of the above categories. In particular, a smartphone can be used as a control object in one application (e.g., an application for navigation or phone search), in another as a data object, as well as interactive or smart weather. It can be used as an ect (e.g., remote interaction with a home energy management system) (Vatamaniuk et al. 2018; Khasanov and Reypnazarov 2019). Therefore, consideration of smart objects in the functional sense of an integrated system is essential.

CPS and IoT concepts are extracted from different environments, especially CPS, mainly from a network engineering and control point of view. CPSs are systems of reciprocal computing elements that control physical objects. In this case, they are the mechanical and electrical systems that are connected to the network using software modules. We use method expertise and details to control distribution and production processes separately.

In addition, the idea of IoT originated mainly in terms of networking and information infrastructure, which includes digital space convergence into the real environment. The word IoT is used as a key word to identify specific facets of Internet and cloud penetration into the physical environment using broadly dispersed devices with built-in identifiers, sensors, and actuators (Miorandi et al. 2012). IIoT, on the other hand, represents the orientation of IoT toward industrial and manufacturing systems.

Despite their different origins, many analyses confirm the compatibility between IoT (IIoT) and CPS concepts. Based on the analyses presented in (Minerva et al. 2015; Katsriku 2018; Greer et al. 2019) and other studies, as well as the fact that IIoT is an integral part of IoT, we have divided this cross-linking integration into six main categories.

Category A. The similarity between CPS and IoT is that they achieve a common result even if they are based on different approaches to achieve the goal. Networking and IoT access, as well as input and CPS management are among the unique features.

Although both IoT and CPS concentrate on improving the link between the cyber world and the physical world through knowledge processing and interactive technologies, they have significant differences: IoT emphasizes networking and aims to connect all in the physical world, because it is an open network platform and infrastructure; CPS emphasizes data sharing and feedback where, in addition to sensing the physical world, the system must provide input and control of the physical world by maintaining a closed system (Greer et al. 2019).

The second statement in this category is due to varying human position in the system. That is, while CPS definitions are more based on person-to-system interactions, IoT definitions emphasize system-to-system interactions and automation aims to reduce human interference.

Based on this category A, we can say that in IIoT the specifics of IoT and CPS are mastered and the similarity between them is exactly described by IIoT (Fig. 3).

Category B. The results of some scientific and analytical studies [e.g., (Ma 2011)] describe the concepts of CPS and IoT as interchangeable without clear distinctions between the two. Such studies point out that the difference between IoT and CPS is not obvious, and that finding a source which makes a clear distinction between these terms is difficult. Most people see these terms as different examples for the same concept and keep using words instead of one another.

IoT is strongly compliant with CPS because IoT is concerned with monitoring items in the real environment, leveraging networking tools, and collecting the information required to control issues that are not done today efficiently. Though IoT had originally addressed applications for detection and tracking, today IoT is increasingly used to

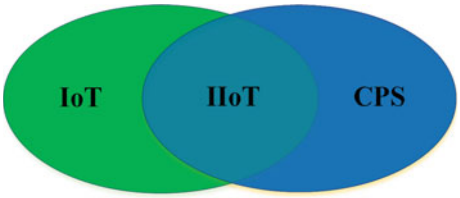


Fig. 3 Category A of integration of IoT, IIoT, and CPS concepts

handle physical environments via the integration of RFID systems and sensor networks.

Based on the above considerations, we have proposed this Category B, which describes IoT and CPS as different names for the same concepts and IIoT as a specific area within them (Fig. 4).

Category C. Two categories of assertions have been put forward to see the concept of CPS as an integral part of IoT. Initially, CPS is described as an IoT platform or building block. The physical world interacts with the virtual world through CPS to form IoT, data, and services.

Second, non-CPS IoT cases exist because, given the limited considering of system-level control, they focus on simple-level controllable and data objects.

Comprehensive IoT concepts may include implementations outside CPS scope, such as IoT-connected home entertainment systems geolocation monitoring networks, or consumer products.

Based on these considerations, we propose categories C (Fig. 5), D (Fig. 6), and E (Fig. 7), which describe CPS as an integral part of IoT and describe the integration of IIoT with them from different perspectives.

Category C CPS and IIoT are considered to be an integral part of IoT and are considered to have significant differences when there are similarities between them (Fig. 5).

Category D. As noted above, CPS and IIoT are considered to be an integral component of IoT in category D, as in category C, but there are no clear differences between them or are not considered significant (Fig. 6).

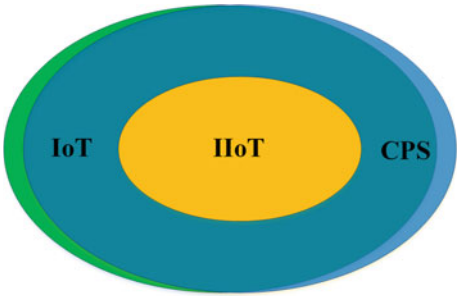


Fig. 4 Category B of integration of IoT, IIoT, and CPS concepts

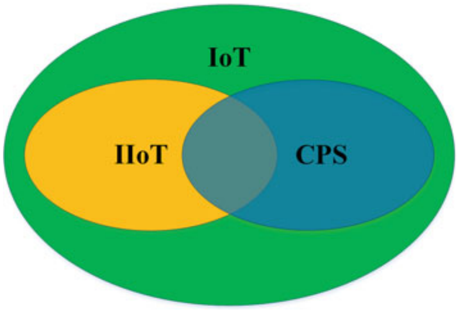


Fig. 5 Category C of integration of IoT, IIoT, and CPS concepts

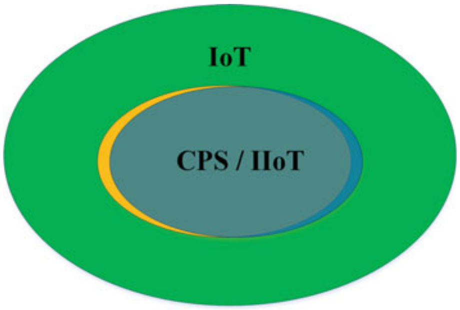


Fig. 6 Category D of integration of IoT, IIoT, and CPS concepts

Category E. In this category, CPS and IIoT are considered to be part of IoT, as in Category C and Category D, and CPSs are also considered to be part of IIoT (Fig. 7).

Category F. We propose this category in (Katsriku 2018; Ma 2011; Stojmenovic and Zhang 2015) based on three main assertions that support the understanding of science-based IoT as a component of CPS. In this case, as in other categories, we considered IIoT as an integral part of IoT (Fig. 8).

The first is to focus more on control in CPS. In systems known as IoT, CPS puts more emphasis on technology control. CPS features are a combination of this system's computational and physical elements and their synchronization, as well as the convergence of computer and information-oriented physical and engineering systems.

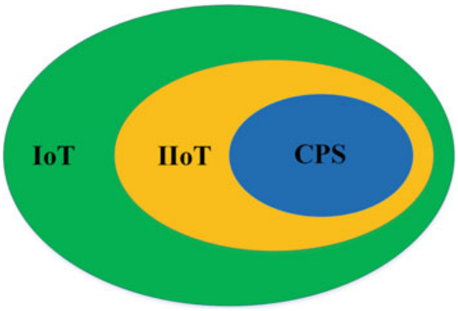


Fig. 7 Category E of integration of IoT, IIoT, and CPS concepts

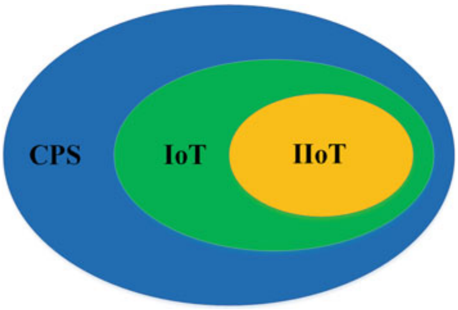


Fig. 8 Category F of integration of IoT, IIoT, and CPS concepts

A significant class of CPS is called IoT (Stojmenovic and Zhang 2015).

In this category, the second confirmation is a confirmation that it may be an IoT CPS platform. The examples below illustrate the depth of prospects within the same general category. Typically, IoT is designed to detect or connect with the physical realm, and to distinguish objects by providing process control information across a network. Cyber-physical systems are usually required to detect and transmit physical data when the Internet is not needed. Such technologies also seek to control complex internal and physical processes and are thus specifically designed to address encounters between humans and machines not protected by IoT (Katsriku 2018).

A third validation in this category—systems that are highly networked but do not have a wide network connection outside the system boundaries—is examples of non-IoT CPS. An example of this would be a broadband autonomous vehicle operating in a confined or externally unconnected environment (Stojmenovic and Zhang 2015).

The categories of integration of IoT, IIoT, and CPS concepts are compared in Table 1.

In general, our analysis from different perspectives and in different categories shows that it is much more difficult to show a clear distinction between CPS, IoT, and IIoT systems. Therefore, it is difficult to give a definite opinion as to which of the categories we have mentioned describes the integration between these concepts. Nevertheless, we propose Category A as the most viable option for the integration of CPS, IoT, and IIoT systems, based on the sound judgment in our research and analysis.

7 Integration of IoT, IIoT, and CPS

Comparisons of IoT, IIoT, and CPS based on different approaches show that the integration between these concepts depends on differences on four main issues (Greer et al. 2019): (1) control: the presence of control at the system level; (2) platform: whether there is an IoT (IIoT) platform for the introduction of CPS or vice versa; (3) Internet connection: what are the requirements for network connection and what tasks are assigned to IP networks in the system; (4) human: the degree of human-machine interaction in the system. In general, a detailed analysis of each element suggests that the evidence presented is not sufficient to draw a clear demarcation line between the concepts of IoT, IIoT, and CPS. The lack of simple and consistent demarcation measures as well as the incremental convergence of meanings thus reinforce consensus on the potential adoption of current IoT, IIoT, and CPS concepts. Some features of the integration of IoT, IIoT, and CPS concepts are presented in Table 2.

CPS pays more attention to control than IoT. In examples such as surveillance smart devices, IoT focuses more on transmitting information streams from sensors rather than monitoring the physical state. Hence, CPS and IoT are considered as separate concepts with significant differences in intelligent environment control. However, given that there are IoT systems that focus on environmental control, they also have commonalities, which we consider to be reflected in the form of IIoT.

The platform includes technology components in the context of communication and information technologies which provide selected services and functions to be used in support of a spectrum of uses. The operating systems are an example of such a platform. Without considering program and applications that perform basic practical tasks for CPS IoT and IIoT, designing a stand-alone platform can lead to limitations and shortcomings that compromise security, reliability, and so on. IoT or CPS must not be viewed at the platform level alone in this respect, but should instead concentrate on the completed functions of entire system. When viewed within a general functional context, platforms or platform-based projects are similar to CPS and IoT, as well as IIoT, and have no differentiating factors, with only minor differences for individual environments. Hence, in terms of platforms for smart environments, CPS and IoT can be seen as almost identical concepts with small differences in integration.

The term IoT literally means connecting things to the Internet. It is clear that for IoT, connecting to the Internet or IP-based network is an important factor. CPS, on the other hand, does not have Internet or IP-oriented restrictions on connections, and different wired and wireless networks based on different standards and protocols can be used to establish connections. So, based on these considerations, CPS and IoT are separate concepts that have significant differences in terms of Internet connectivity. However, today, in smart systems that are considered to be based on IoT solutions, protocols such as named data networking (NDN) and unstructured supplementary service data (USSD) are used instead of TCP/IP protocols to establish connections

Table 1 Categories of integration of IoT, IIoT, and CPS concepts

	IoT	IIoT	CPS
Category A	An independent system that differs from CPS	Convergence of IoT and CPS, subsystem	An independent system that differs from IoT
Category B	Same concept with CPS	A special area of IoT, subsystem	Same concept with IoT
Category C	An independent system that includes IIoT and CPS	A special area of IoT, subsystem	A special area of IoT, subsystem
Category D	An independent system that includes IIoT and CPS	A special area of IoT, subsystem	A special area of IoT, a different name for IIoT
Category E	An independent system that includes IIoT and CPS	A special area of IoT, subsystem	A special area of IIoT, subsystem
Category F	A special area of CPS, subsystem	A special area of IoT, subsystem	An independent system that includes IoT and IIoT

Table 2 Features of integration of IoT, IIoT, and CPS concepts

	IoT	IIoT	CPS
Control	Little attention	Relatively much attention	Great attention
Platform	Need to pay attention to the platform as well as the apps and applications	Need to pay attention to the platform as well as the apps and applications	Need to pay attention to the platform as well as the apps and applications
Internet connection	Basic requirement	Basic requirement	Other networks from the Internet can also be used for communication
Human intervention	Minimize human intervention	Minimize human intervention	New opportunities for human-machine communication

(Puthal et al. 2018). Based on these facts, CPS and IoT are integrated in terms of connectivity for smart environments, and IIoT are the systems that are at the heart of this integration.

The next issue in defining the integration between the concepts of IoT, IIoT, and CPS is to clearly describe the position of users (human) and operators in these systems. CPS refers to smart machine- and physical-capable devices that can communicate with people through several different methods. IoT, on other hand, are intelligent systems with computing and physical capabilities that aim for minimal human intervention in the production, exchange, and consumption of information. However, systems can be IoT or CPS, depending on automation level and human interaction. This is because none of the definitions given to CPS deny the complete automation of the system, nor do the IoT definitions deny human involvement in the system. Hence, the approach in terms of the degree of automation and human intervention shows that there are no obvious differences between the concepts of IoT, IIoT, and CPS, and presents them as integrated concepts.

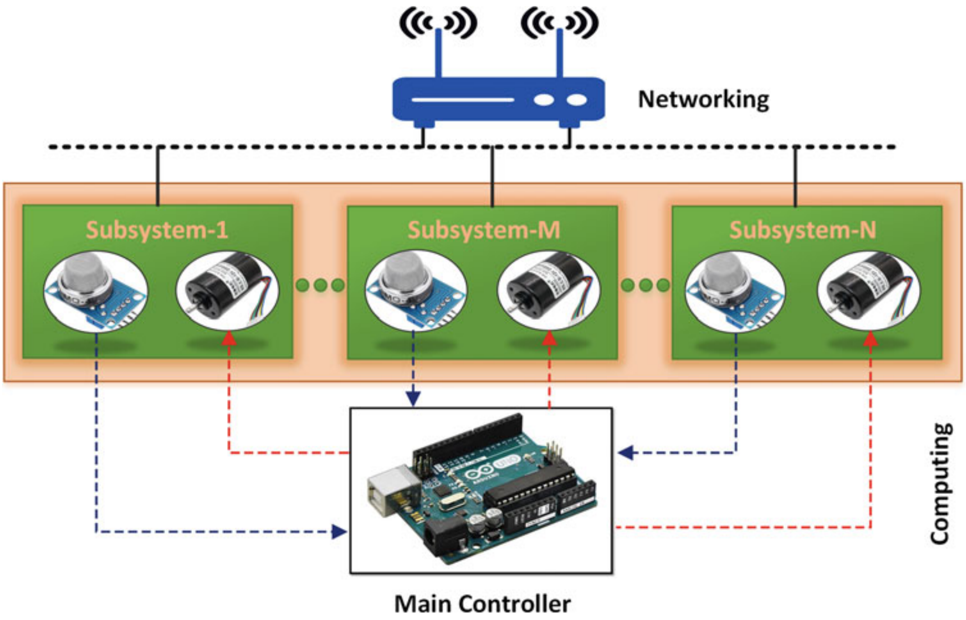
In general, the above problems for distinguishing the concepts of IoT, IIoT, and CPS indicate that there are no reliable differences, but rather that they are deeply integrated concepts. The lack of clear and consistent measurements that distinguish the concepts of CPS and IoT allows us to conclude that these concepts are very similar systems with small differences, and that this similarity is manifested as IIoT.

8 Control System of Integrated IoT, IIoT, and CPS

The integrated IoT/IIoT/CPS control system plays an important role in manufacturing and industrial enterprises functioning critical infrastructure. Like the control systems of many other systems, the control systems of these systems are divided into decentralized, centralized, and hierarchical types of control, depending on the overall structure of the system (Scattolini 2009).

Figure 9 presents a schematic diagram of a centralized IoT/IIoT/CPS control system that uses a centralized controller to control and monitor several subsystems. Every subsystem can be described as a set of sensors and actuators. The sensors fix the operating status of the system and transmit information to central controller. This central controller makes a decision regarding control and transmits the control signals to the actuators. The collection, analysis of fixed data, and the transmission of commands to all objects are carried out by a central controller. One example of a

Fig. 9 Structure of a centralized control system



centralized control structure is SCADA. Complete scientific-theoretical analysis of centralized control systems of IoT/IIoT/CPS can be obtained from (Xu et al. 2018; Hunzinger 2017; Alhebshi et al. 2018; Shahzad et al. 2017).

Figure 10 shows a block scheme of decentralized control system in IoT/IIoT/CPS, and the main difference from a centralized control system is that it has separate controllers for each subsystem. These controllers control the performance of each subsystem.

One example of decentralized control systems is distributed control systems (Xu et al. 2018). Distributed control systems are typically designed to control manufacturing processes. To do this, distributed control systems can control several subsystems at a high level and control processes within the system (Stouffer et al. 2015). Typically, controllers have been implemented in distributed control systems to provide the control system with specific parts and manufacturing processes, and the controllers operate together to perform manufacturing processes. Complete scientific and theoretical analysis of decentralized control systems of IoT/IIoT/CPS can be obtained from (Stouffer et al. 2015; El-Shafei et al. 2017).

Figure 11 shows a block scheme of a hierarchical control system in IoT/IIoT/CPS, which is mainly used to operate in complex and large manufacturing systems using multi-level structure mechanisms. In this case, the lower level consists of local controllers that perform control functions in direct communication with the subsystems. The results obtained and the results of the control are transmitted to a higher level for monitoring control or for effective coordination of large systems (Scattolini 2009).

Table 3 provides comparative data on the properties of decentralized, centralized, and hierarchical control systems.

In various industrial and manufacturing systems, different control systems types serve different control requirements. Integrating the various control systems can also be efficient, effective, and manageable to work in large-scale and complex production systems. As an example of an electricity generation system, electricity is generated from many types of power plants, where distributed control systems can control the operating facilities. SCADA can also be used to monitor different power plants and to provide a high degree of coordination and control (Lü et al. 2017). Through taking advantage of both, the combination of distributed control systems and SCADA will improve the efficiency of power generation, distribution, and transmission. Full scientific and theoretical analysis of the IoT/IIoT/CPS hierarchical control systems can be obtained from (Lü et al. 2017; Selişteanu et al. 2018).

9 Networking in Integrated IoT, IIoT, and CPS

There are many different technology-based options for building data transmission networks between sensors (actuators) and applications (mobile or web) through the IoT, IIoT, and CPS platforms. The following is a general analysis of these technologies.

Wired or short radius wireless networks. The first method is to connect the wired sensors, and the second choice is to use wireless networks of short range. However,

Fig. 10 Structure of a decentralized control system

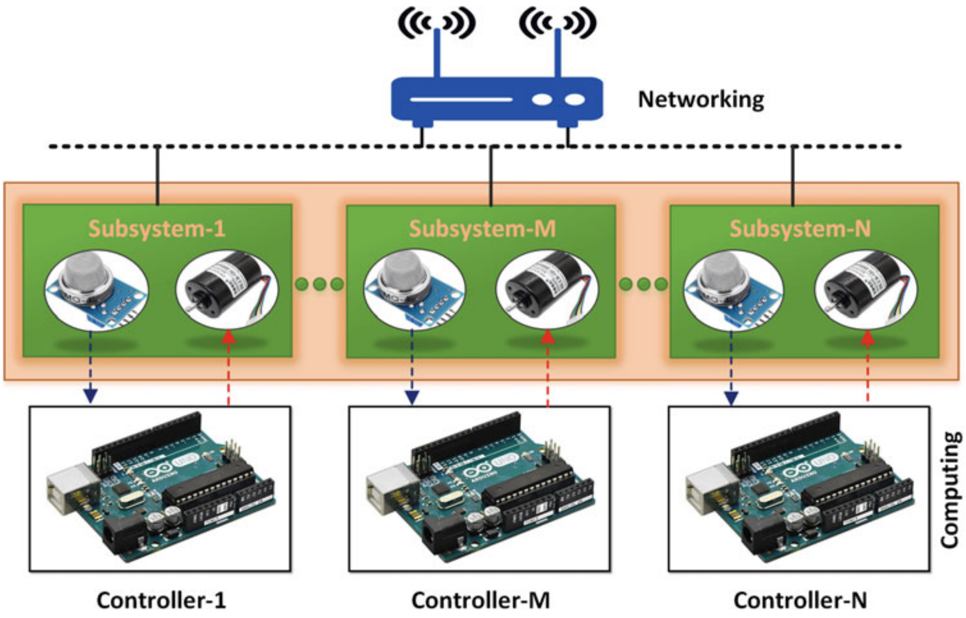
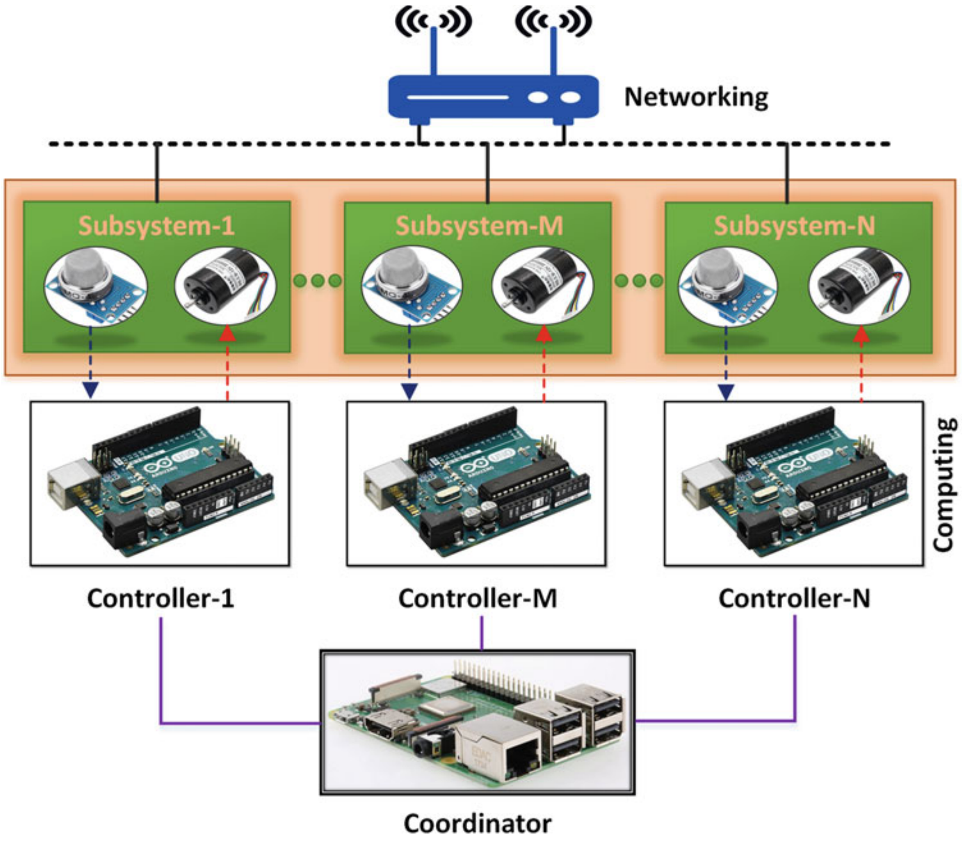


Fig. 11 Structure of the hierarchical management system



the disadvantages of both options are that they do not provide global opportunities and are limited. By short-range wireless networks, we can understand the following (Khujamatov et al. 2020):

- Networks based on Wi-Fi technology. The disadvantages of this technology are the high energy requirements, the lack of battery capacity, and the lack of good adaptation to manufacturing environments.

Table 3 Comparison of decentralized, centralized, and hierarchical control systems

	Centralized control	Decentralized control	Hierarchical control
Number of subsystems	Relatively little	Relatively many (several)	Many
Requirements for controller parameters	Very big	Small	Small, for basic controller is huge
Energy efficiency	High	Low	High
Time efficiency	Low	High	High

- Networks based on ZigBee, Z-Wave, Bluetooth technologies.

M2M networks. The only global solution to remotely connect objects (devices, cars, vehicles, etc.) is to install SIM cards in the devices and use 2G/3G/4G mobile networks of telecommunications operators. The main problems of these technologies, commonly known as machine to machine (M2M), are:

- High cost of equipment;
- Very high energy demand;
- Relative cost of connection.

Due to this, it is difficult to connect small and powerless objects to M2M. Even if you make the connection, the size of the sensor may be larger than the size of the object (Singh et al. 2020).

LPWAN. Low-power wide area networks (LPWAN) technology has been developed due to existing problems in wired or short-range wireless networks as well as M2M networks. The purpose of this technology is to provide sensors with the following features for connection to objects:

- Cheap;
- Small size;
- Long battery life;
- Communication at very low data rates (connection costs a few cents per month).

The main representatives of LPWAN for IoT, IIoT, and CPS projects are: SigFox and LoRaWAN technologies. NB-IoT technology should also be mentioned.

SigFox and LoRaWAN. As mentioned above, the most widely used network technologies in the area we are researching are SigFox and LoRa technologies. Although based on different methods, both technologies are technically equivalent. These technologies operate on the frequency band of free industrial, scientific, and medical (ISM) so no license is required.

The working principle of these technologies is that the sensor is often in a sleeping state (to save battery) and wakes up from time to time to transmit measured data, usually every 10 min. Data packets are conveyed across all connected gateways. Such information is then forwarded to the IoT network for data processing over the Internet. While SigFox is based on a global network that supports roaming, LoRaWAN is based on building a private network.

Table 4 provides a comparative analysis of key performance indicators of SigFox and LoRaWAN technologies.

NB-IoT. Narrow band IoT (NB-IoT) is a solution developed by traditional GSM operators in response to LPWAN technology solutions. This technology is a specialized version of 4G (LTE) technology with limited bandwidth. This technology involves improving the current network. If we assume that this solution can cover the country's network on a global scale, energy consumption and the cost of sensors can also be much higher. In addition, it is not possible to build private networks on the basis of NB-IoT. This is an interesting alternative technology for IoT, IIoT, and CPS networks in any case, but is not promising for future requirements.

5G. The number of networked devices is rising day after day. At the same time, the development of 5G networks is becoming one of the most important. The 5G standard is a new generation of mobile networks based on the IMT-2020 standard, in which the connection speed can be up to 7 Gbps (Lü et al. 2017). The launch of this new generation of mobile communications has been great news for the IoT, IIoT, and CPS market.

10 Computing in Integrated IoT, IIoT, and CPS

The rapid development of IoT, IIoT, and CPS has posed a number of challenges in the development of cloud computing solutions. These difficulties are mainly due to the fact that large amounts of data are transmitted to the cloud, high latency in communication, and the inability of this model to be used in some areas where rapid response to an event is required (Skala et al. 2015).

The application of IoT, IIoT, and CPS solutions in manufacturing and industry has contributed to technology

Table 4 Comparison of SigFox and LoRaWAN technologies

	LoRaWAN	SigFox
Networking principle	An open standard (LoRa Alliance) for an IoT network. Everybody can deploy and operate a public or private LoRaWAN network	One global operator. Available today in more than 30 countries
Uplink (data from the device to the network)	140 messages of 12 bytes per day	140 messages of 12 bytes per day
Downlink (data from the network to the device)	More flexible	4 messages per day
Strengths	Possibility to build its own LoRaWAN private networks	A global network (with roaming "by design")

rethinking through the implementation of edge, fog, and cloud computing architectures. Such technologies enable them to leverage the many computing and data storage possibilities.

Although edge, fog, and cloud computing all look so similar to each other, they work as different layers in the IoT, IIoT, and CPS architecture and have some differences and complement each other in terms of computational capabilities (Fig. 12).

Cloud computing is understood as a model for the provision and use of ICTs to provide remote access to a number of popular computing resources in the form of Internet services.

This can be split into two parts of this computer system: client devices and servers. Cloud computing services also come in three types: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) (Skala et al. 2015).

The use of this technology in manufacturing and industrial automation offers useful opportunities for performance, connectivity, scalability, sensor-to-machine communication, and increases data processing and storage capabilities.

Fog computing is a computing system used to get the capabilities of cloud computing closer to the network. This is a decentralized architecture of computing, in which data is distributed between data sources and cloud. That is, it is a horizontal architecture which distributes to devices resources and services stored in the fog. So, fog computing can be understood as an intermediate layer that controls the connection between cloud and edge of network.

The main difference among fog and cloud computing is that while cloud computing is a centralized, fog computing is a decentralized distributed infrastructure.

Edge computing is located at the boundary between an industrial or manufacturing facility and a network. In this architecture, data from the source is processed close to the source without being sent over long distances (to the cloud or other centralized processing systems). It increases data transfer to a centralized system by reducing the distance and time of data transmission, as well as the speed and efficiency of devices and applications.

Here the data is stored, the key difference between edge computing and fog computing. Edge computing is usually performed on sensor modules or gateways which are close to the sensors.

Benefits of edge computing are optimization of the connection and improved response time. This also improves security by implementing encryption quite near to the center of the network.

The edge computing, however, has a restricted scope of operation focused on particular and predefined processing patterns at the end of the network.

The following table compares the cloud, fog, and edge computational characteristics (Table 5).

In practice, edge computing is always used as a complementary solution to cloud. The fog computing may not be used by edge computing however. Fog computing also usually involves cloud computing, though edge computing does not.

IoT, IIoT, and CPS are a growing field requiring more effective ways of managing processing and transmission of data.

Use of edge, fog, or computing systems to better analyze data from IoT devices would accelerate the global transition to Industry 4.0.

11 Security Issues of Integrated IoT, IIoT, and CPS

In IoT, IIoT, and CPS, the security issues are one of the most complex problems compared to other problems (Kouicem et al. 2018).

Those systems' security issues are different from Internet security and security of other networks. It includes access rights, confidentiality, verification, authorization, system configuration, control of data storage and data management, and more. Custom security protocols, simplified

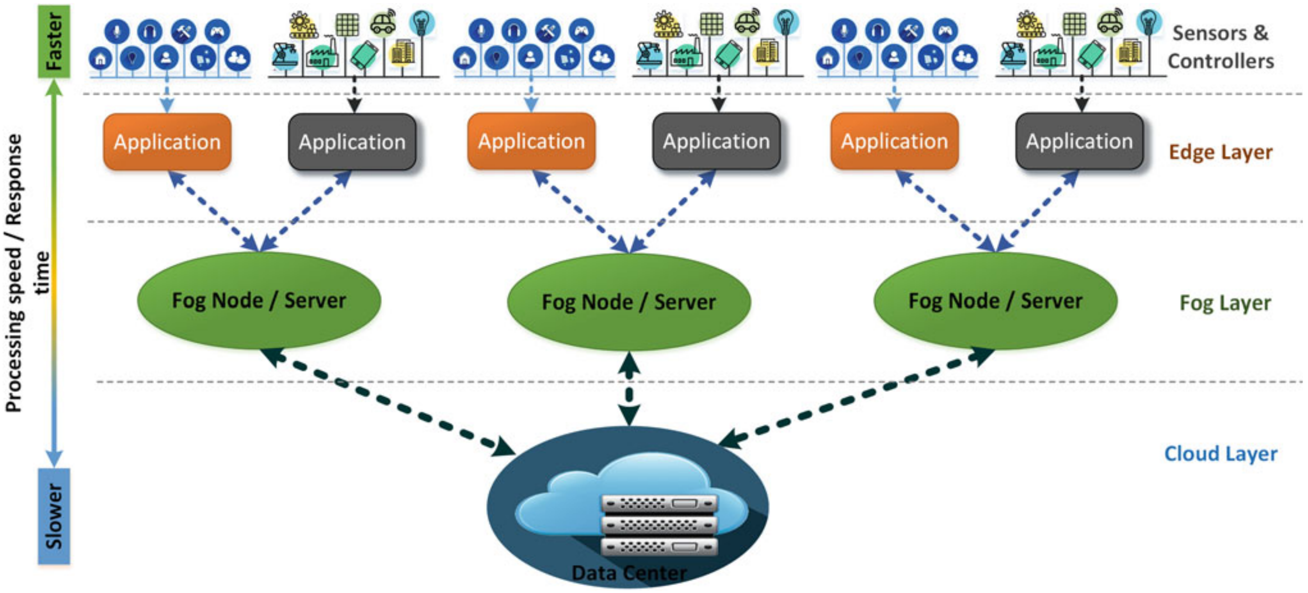


Fig. 12 Computing in IoT/IIoT/CPS

Table 5 Comparison of cloud, fog, and edge computing

	Cloud	Fog	Edge
Architectures	Centralized	Distributed	Distributed
Computing capability	Bigger	Smaller	Small
Data processing	Far from the source of information	Close to the source of information	In the source of information
Latency	High	Medium	Low
Connectivity	Via Internet	Various protocols and standards	Directly connection
Analysis term	Long term	Medium term	Short term
Security	Weaker	Stronger	Strongest

cryptography, simplified authentication, blockchain, etc., are modern trends in building the secure architecture of IoT, IIoT, and CPS (Puthal et al. 2018; Sehgal et al. 2020). Blockchain-based approaches are recognized as an effective solution for encrypting and decrypting large amounts of data in smart environments.

In Kouicem et al. (2018), Kumar and Sukumar (2018), Elhoseny et al. (2018), Albalas et al. (2018) on crypto-technology-based solutions, in Kouicem et al. (2018), Srinivas et al. (2018), Yang et al. (2018), Cui et al. (2018) on authentication-technology-based solutions provide scientific and theoretical-analytical data of security in IoT, IIoT, and CPS systems of industrial and industrial enterprises.

A blockchain is an increasing collection of records which are cryptographically related. It consists of a blockchain, each block having a previous block cryptographic hash (Puthal et al. 2018). The blockchain is thus impervious to change of the data. Blockchain is a new technology consisting of a secure database which contains all the operations that the entities involved in the system have created.

The results and analyses of recent blockchain-based research on security in industrial and industrial IoT, IIoT, and CPS systems are presented in Puthal et al. (2018), Li (2017, 2018), Sagirlar et al. (2018).

Over time, the databases of CPS, IoT, and IIoT systems have become much larger. Therefore, confidentiality is required to ensure the security of this system information. The results of research and theoretical-analytical data on methods of data confidentiality in these systems are presented in Ren et al. (2018), Du et al. (2018), Ullah et al. (2017).

In general, the cryptography and authentication methods of IoT, IIoT, and CPS systems should have simpler features than other traditional cryptography and authentication methods. To that network power consumption, many devices now use small-scale algorithms for encryption, decryption, or authentication.

Blockchain is the ultimate solution that solves some of the issues in the traditional security solutions of IoT, IIoT, and CPS applications.

12 Conclusion and Future Work

In this chapter, IoT, IIoT, and CPS are compared in terms of origin, application, architecture, characteristics, and the degree of integration between them is determined. In determining the degree of integration between these systems, they took into account the similarities and differences in approaches and solutions to the issues of control, platform, Internet access, and human intervention. The similarities between IoT, IIoT, and CPS were compared from different perspectives and studied in six categories. In general, approaches from different perspectives and analyses across different categories show that it is much more difficult to make a clear distinction between CPS, IoT, and IIoT systems. Therefore, it is difficult to give a definite opinion as to which of these categories describes the integration between these concepts. However, based on the findings of the research and analysis, Category A has been proposed as the most viable option for integrating IoT, IIoT, and CPS systems.

It also provides analytical data on the industrial revolution and Industry 4.0 technologies, CPS, IoT, and IIoT for smart environments, their origins, development trends, definitions, architectures, components, applications, and characteristics. In integrated IoT, IIoT, and cyber-physics systems, control, networking, computing, and security issues were studied.

Based on the analysis of this work, we aim to conduct research in our future work to address the following issues:

- Creation of methods and algorithms for increasing of efficiency and safety of data processing in IoT, IIoT, and CPS;
- Development of data processing method and algorithms for in IoT-enabled smart grid based on edge computing and blockchain.

References

Ahanger, T. A., & Aljumah, A. (2019). Internet of Things: a comprehensive study of security issues and defense mechanisms. *IEEE Access, 7,* 11020–11028.

Ahmadi, A., Sodhro, A., Cherifi C., Cheutet, V., & Ouzrout, Y. (2018). *Evolution of 3C Cyber-Physical Systems Architecture for Industry 4.0.*

Albalas, F., Al-Soud, M., Almomani, O., & Almomani, A. (2018). Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography. *The International Arab Journal of Information Technology, 15*(3A, Special Issue)

Alhebshi, F., Alnabilsi, H., Alzebaidi, J., Bensenouci, A., Brahimi, T., & Bensenouci, M.-A. (2018). Monitoring the operation of transmission line in a smart grid system through IoT. In *2018 15th Learning and Technology Conference (L&T)* (pp. 139–146). IEEE.

Anavangot, V., Menon, V.G., & Nayyar, A. (2018, November). Distributed big data analytics in the Internet of signals. In *2018 International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 73–77). IEEE.

Batth, R. S., Nayyar, A., & Nagpal, A. (2018, August). Internet of robotic things: driving intelligent robotics of future-concept, architecture, applications and technologies. In 2018 4th International Conference on Computing Sciences (ICCS) (pp. 151–160). IEEE.

Cui, H., Deng, R. H., Liu, J. K., Yi, X., & Li, Y. (2018). Server-aided attribute-based signature with revocation for resource-constrained industrial-internet-of-things devices. *IEEE Transactions on Industrial Informatics, 14*(8), 3724–3732.

Du, M., Wang, K., Chen, Y., Wang, X., & Sun, Y. (2018). Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things. *IEEE Communications Magazine, 56*(8), 62–7.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. In *Neural Computing and Applications.* Springer

El-Shafei, M. A., El-Hawwary, M. I., & Emara, H. M. (2017). Implementation of fractional-order PID controller in an industrial distributed control system. In *2017 14th International Multi-Conference on Systems, Signals & Devices (SSD)* (pp. 713–718). IEEE.

Greer, C., Burns, M., Wollman, D., & Griffor, E. (1900). Cyber-physical systems and Internet of Things. *NST Special Publication, 202,* 52. https://doi.org/10.6028/NIST.SP.1900-202.

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). *Cyber-physical systems and internet of things* (p. 52). NST Special Publication, 1900–202. https://doi.org/10.6028/nist.sp.1900-202

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the energy sector. *Energies, 13*, 494. https://doi.org/10.3390/en13020494.

Hunzinger, R. (2017). SCADA fundamentals and applications in the IoT. In *Internet of Things and Data Analytics Handbook* (pp. 283–293).

Ibarra-Esquer, J. E., González-Navarro, F. F., Flores-Rios, B. L., Burtseva, L., & Astorga-Vargas, M. A. (2017). Tracking the evolution of the internet of things concept across different application domains. *Sensors, 17*(6), 1379. http://www.doi.org/10.3390/s17061379

Khujamatov, Kh. E. Khasanov, D. T., & Reypnazarov, E. N. (2019). Modeling and research of automatic sun tracking system on the bases of IoT and Arduino UNO. In *International Conference on Information Science and Communications Technologies ICISCT 2019*, Tashkent, Uzbekistan. https://doi.org/10.1109/icisct47635.2019.9011913

Khujamatov, Kh. E., Khasanov, D. T., & Reypnazarov, E. N. (2019). Research and modelling adaptive management of hybrid power supply systems for object telecommunications based on IoT. In *International Conference on Information Science and Communications Technologies ICISCT 2019*, Tashkent, Uzbekistan. https://doi.org/10.1109/icisct47635.2019.9011831

Khujamatov, K., Ahmad, K., Reypnazarov, E., & Khasanov, D. (2020). Markov Chain based modeling bandwith states of the wireless sensor networks of monitoring system. *International Journal of Advanced Science and Technology*, *29*(4), 4889–4903. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/24920

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 4*(141), 199–221.

Krishnamurthi, R., Nayyar, A., & Solanki, A. (2019). Innovation opportunities through internet of things (IoT) for smart cities. In *Green and Smart Technologies for Smart Cities* (pp. 261–292). CRC Press.

Kumar, A., & Nayyar, A. (2020). si 3-Industry: A sustainable, intelligent, innovative, internet-of-things industry. In: *A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development* (pp. 1–21). Springer, Cham.

Kumar, K. S., & Sukumar, R. (2018). *Achieving energy efficiency using novel scalar multiplication based ECC for android devices in Internet of Things environments*. Springer

Lee, E. A., & Seshia, S. A. (2016). *Introduction to embedded systems: A cyber-physical systems approach*. London: MIT Press Publ.

Li, Z., et al. (2017) *Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things* (pp. 1551–3203). IEEE.

Li, R. et al. (2018) *Blockchain For Large-Scale Internet of Things Data Storage and Protection*. IEEE.

Liu, Chao, & Jiang, Pingyu. (2016). A cyber-physical system architecture in shop floor for intelligent manufacturing. *Procedia CIRP, 56,* 372–377. https://doi.org/10.1016/j.procir.2016.10.059.

Lü, Z., Lü, Y., Yuan, M., & Wang, Z. (2017). A heterogeneous large-scale parallel SCADA/DCS architecture in 5G OGCE. In *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)* (pp. 1–7). IEEE.

Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer science and Technology, 26*(6), 919–924. https://doi.org/10.1007/s11390-011-1189-5.

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative, 1*, 1–86. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf

Miorandi, D., Sicari, S., Pellegrini, F., & Chlamta, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016.

Namiot, D. (2015). On big data stream processing. *International Journal of Open Information Technologies, 3*(8), 48–51

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 217–243). Academic Press.

Park, K.-J., Zheng, R., & Liu, X. (2012) Cyber-physical systems: Milestones and research challenges. *Editorial Computer Communications, 36*(1), 1–7. https://doi.org/10.1016/j.comcom.2012.09.006

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine, 7*(2), 18–21.

Ren, H., Li, H., Dai, Y., Yang, K., & Lin, X. (2018). Querying in internet of things with privacy preserving: Challenges, solutions and opportunities. *IEEE Network, 32*(6), 144–51.

Sagirlar, G., Carminati, B., & Ferrari, E. (2018). AutoBotCatcher: blockchain-based P2P botnet detection for the internet of things. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing*.

Sanislav, T., et al. (2017). Multi-agent architecture for reliable cyber-physical systems (CPS). In *2017 IEEE Symposium on Computers and Communications (ISCC)* (pp. 170–175).

Scattolini, R. (2009). Architectures for distributed and hierarchical model predictive control–a review. *Journal of Process Control, 19* (5), 723–731.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Selişteanu, D., Roman, M., Şendrescu, D., Petre, E., & Popa, B. (2018) A distributed control system for processes in food industry: Architecture and implementation. In *2018 19th International Carpathian Control Conference (ICCC)*. IEEE.

Shahzad, A., Kim, Y.-G., & Elgamoudi, A. (2017). Secure IoT platform for industrial control systems. In *2017 International Conference Platform Technology and Service (PlatCon)* (pp. 1–6). IEEE.

Siddikov, I Kh, Sattarov, Kh A, & Khujamatov, Kh E. (2016). Research of the influence of nonlinear primary magnetization curves of magnetic circuits of electromagnetic transducers of the three-phases current. *Universal Journal of Electrical and Electronic Engineering. Horizon Research Publishing Corporation, USA, 4*(1), 29–32. https://doi.org/10.13189/ujeee.2016.040104.

Siddikov, I. Kh., Sattarov, Kh. A., & Khujamatov, Kh. E. (2017). Modeling of the transformation elements of power sources control. In *International Conference on Information Science and Communications Technologies (ICISCT) Applications, Trends and Opportunities*, 2nd, 3rd and 4th of November 2017, Tashkent, Uzbekistan. https://doi.org/10.1109/icisct.2017.8188581

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of Things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth, 2,* 191.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020). Internet of Things in pharma industry: Possibilities and challenges. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 195–216). Academic Press.

Skala, K., Davidovic, D., Afgan, E., Sovic, I., & Sojat, Z. (2015). Scalable distributed computing hierarchy: Cloud, fog and dew computing. *Open Journal of Cloud Computing (OJCC)., 2*(1), 16–24. https://doi.org/10.19210/1002.2.1.16.

Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In Handbook of Research on Big Data and the IoT (pp. 379–405). IGI Global.

Srinivas, J., Das, A. K., Wazid, M., & Kumar, N. (2018). Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, 1545–5971. IEEE.

Stojmenovic, I., & Zhang, F. (2015). Forward: Inaugural issue of 'cyber-physical systems'. *Cyber-Physical Systems, 1*(1), 1–4. https://doi.org/10.1080/23335777.2015.970764.

Stouffer, K., Falco, J., & Scarfone, K. (2015). Guide to industrial control systems (ICS) security. *NIST Special Publication, 800*(82).

Tanwar, S. (2020). Fog data analytics for IoT applications—next generation process model with state-of-the-art technologies. *Studies in Big Data, Springer International Publishing, 76,* 1–497.

Ullah, I., Shah, M. A., Wahid, A., Mehmood, A., & Song, H. (2017). *ESOT: A new privacy model for preserving location privacy in Internet of Things*. Springer

Vatamaniuk, I. V., Malov, D. A., & Levonevskii, D. K. (2018). Modeling the QoE estimation for services of the cyberphysical intelligent space. In *Proceedings of the 2018 IEEE Northwest Russia Conference on Mathematical Methods in Engineering and Technology (MMET NW)* (pp. 436–439).

Wu, Yanpeng, Wu, Ying, Guerrero, Josep, Vasquez, Juan, Palacios-García, Emilio, & Guan, Yajuan. (2020). IoT-enabled microgrid for intelligent energy-aware buildings: a novel hierarchical self-consumption scheme with renewables. *Electronics, 9,* 550. https://doi.org/10.3390/electronics9040550.

Xu, H., Yu, W., Griffith, D., & Golmie, N. (2018). A survey on industrial internet of things: A cyber-physical systems perspective. *IEEE Access*, pp. 1–1. https://doi.org/10.1109/access.2018.2884906.

Yang, Y., Liu, X., & Deng, R. H. (2018). Lightweight break-glass access control system for healthcare Internet-of-Things. *IEEE Transactions on Industrial Informatics., 14*(8), 3610.

Yeboah-ofori A., Abdulai J., & Katsriku, F. (2018). *Cybercrime and risks for cyber physical systems: A review*. Preprints 2018. https://doi.org/10.20944/preprints201804.0066.v1

Event and Activity Recognition in Video Surveillance for Cyber-Physical Systems

Swarnabja Bhaumik, Prithwish Jana
and Partha Pratim Mohanta

Abstract

In this chapter, we aim to aid the development of Cyber-Physical Systems (CPS) in automated understanding of events and activities in various applications of video-surveillance. These events are mostly captured by drones, CCTVs or novice and unskilled individuals on low-end devices. Being unconstrained in nature, these videos are immensely challenging due to a number of quality factors. We present an extensive account of the various approaches taken to solve the problem over the years. This ranges from methods as early as Structure from Motion (SFM) based approaches to recent solution frameworks involving deep neural networks. We show that the long-term motion patterns alone play a pivotal role in the task of recognizing an event. Consequently each video is significantly represented by a fixed number of key-frames using a graph-based approach. Only the temporal features are exploited using a hybrid Convolutional Neural Network (CNN + Recurrent Neural Network (RNN)) architecture. The results we obtain are encouraging as they outperform standard temporal CNNs and are at par with those using spatial information along with motion cues. Further exploring multistream models, we conceive a multi-tier fusion strategy for the spatial and temporal wings of a network. A consolidated representation of the respective individual prediction vectors on video and frame levels is obtained using a biased conflation technique. The fusion strategy endows us with greater rise in precision on each stage as compared to the state-of-the-art methods, and thus a powerful consensus is achieved in classification. Results are recorded on four benchmark datasets widely used in the domain of action recognition, namely Columbia Consumer Videos (CCV), Human Motion Database (HMDB), UCF-101 and Kodak's Consumer Video (KCV). It is inferable that focusing on better classification of the video sequences certainly leads to robust actuation of a system designed for event surveillance and object cum activity tracking.

Keywords

Activity recognition • Cyber-physical systems • Event classification • Motion and video analysis • Spatio-temporal features

1 Introduction

Images and motion pictures were until a point of time, a manifestation of lucid art and complex ideas that only humans could appreciate and analyze, owing to their priceless gifts of vision and cognition. The fact that even computers could comprehend and obtain a semantic and high-level understanding of what digital images and videos had to offer was a dream unrealized before the advent of the computer vision. At present, computer vision is an extensive field of study, and an active domain of research. In this chapter, we deal with the problem of event recognition. The goal of event recognition is to understand the various diverse *events* such as Birthday, Graduation, Wedding-Reception, and *activities* like Dancing, Horse-Riding, Walking and so on. These events and activities are mostly captured by drones, CCTVs or novice and unskilled individuals on low-end capturing devices. As a result, these videos are often found to have inadequate brightness, jitter and, are temporally redundant on a number of occa-

---

S. Bhaumik
Department of Computer Science and Engineering, Meghnad Saha Institute of Technology, Kolkata, India
e-mail: swarnabjazq22@gmail.com

P. Jana
Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India
e-mail: pjana@ieee.org

P. P. Mohanta (✉)
Electronics and Communication Sciences Unit, Indian Statistical Institute, Kolkata, India
e-mail: partha.p.mohanta@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_4

sions. Camera movement and cluttered background are also prevalent. These videos are termed as ‘unconstrained’ video. The present work focuses on the classification of unconstrained videos abundantly available either in the prerecorded form in online video-sharing platforms such as YouTube and Facebook, or in real-time. Being unconstrained in nature, these videos have often posed a challenge to researchers. On the other hand, the rising demand for retrieval of high-level information based on the content of the video, the problem of event recognition has garnered much interest. This brings us at a confluence of the broad streams of machine vision and artificial intelligence (with sub-fields being machine learning and deep learning) to deal the problem in real-life scenarios. With a better and enforced automated understanding of surrounding events, a number of significant problems such as unmanned video surveillance and tracking in various domains including sports, defense, and other related areas, can also be addressed. The challenge is to represent each of these complex events or activities with their underlying unique structure/pattern. With the prevalence and access of Cyber-Physical Systems (CPS), this progress in comprehending complex activities using patterns can be further well realized and actuated, thereby allowing an interactive exchange between the physical and software components of the solution.

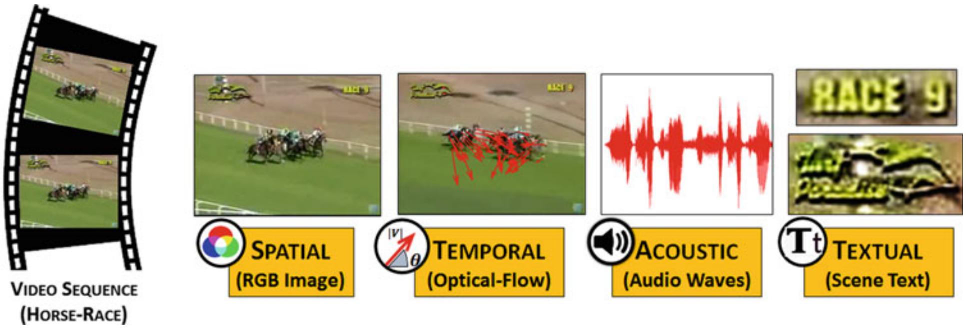
Automatic Video Surveillance (AVS) is a sub-field of scene understanding. AVS systems are specifically employed to identify human activities that are apparently abnormal or pose to be a threat, in the backdrop of a particular event. For example, bending down before jumping may pose to be a threat (suicidal behaviour) at a rapid-transit platform, but not (warm-up exercise) at an athletics’ arena. CCTVs are installed at specific positions and the captured video data is constantly monitored by a software. Two purposes are served with the help of CCTV. Firstly, warnings (person roaming outside an ATM before attempting robbery, using abusive language before indulging in an aggressive fight, etc.) that led to a abnormal situation in the past, are useful for training purposes. It’s indeed an effective way of learning for the authority, such that they can take necessary measures to prevent *similar* events actually takes place in the future. Thus, the classification model can adapt itself through learning past instances. Secondly, when surveillance is done in real-time, the emergency services can be automatically alerted of a potential risk by alarms, SMS or direct phone calls from the software system. Such systems do not necessitate a human operator to be present 24 × 7 before a camera, and thus eliminates out chances of overlook due to human-errors and operator fatigue. Hence, it can be ensured that whatever be the hardware configuration, the back-end software in an AVS system must perform effectively towards both the event classification and the human-activity recognition in real time. To successfully achieve both of these tasks (event classification and the human-activity recognition) efficient extraction of all the information (spatial, temporal, audio and text) from the video and their suitable representation are of prime importance. Thus, efficient exploitation of multimodal information leads to the correct identification of body-languages and human activities in a surveillance video.

1.1 Mathematical Representation and Multimodality Concepts

A video can be represented as a sequence of frames, $\{f_k\}$, where $k \in [1, N]$ denotes the order (or, time) of appearance. Here, N is the total number of frames in the video. Thus, considering x and y to be the horizontal and vertical position of a pixel within a frame, any pixel in a video can be referenced through a 3-D coordinate (x, y, k). Now, videos typically contains multimodal information and they can be exploited efficiently through one/more of four major channels. These are elaborated subsequently, and shown in Fig. 1.

- ***Spatial***. (i.e. space) Also known as the visual channel, this characterizes all the intra-frame information, i.e. within a particular video-frame f_k and at a particular time instance k. Such apparent and single-image information can be perceived through image-processing methodologies, that ranges from inspecting RGB intensity values to localization of a certain object-of-interest.
- ***Temporal***. (i.e. time) This channel characterizes the inter-frame correlations between successive frames at running time instances. Conventional image processing techniques

Fig. 1 The most common multimodal features, that are readily available from a video



are not suitable for computing such correlations between a pair of frames. However, a special video processing concept such as optical-flow needs to be exploited to capture information from a sequence of frames. This channel proves to be helpful in tracking iso-intensity pixels belonging to the same object, with passage of time.

- ***Acoustic***. (i.e. sound) This channel refers to the auditory signals, that are heard while playing a video. The audio signal refers to background music (e.g. national anthem or birthday song), communication within two entities/groups (e.g. human chit-chatting, wolves howling), etc. Automatic speech recognition from an ongoing conversation can often prove to be highly useful in the context of scene understanding.
- ***Textual***. In some cases acoustic conversation may not be recognizable as it is spoken in an unknown language or gibberish in nature. In such situations, text appearing on the video frame and/or subtitles can be extracted and recognized very efficiently by applying some classical image processing and classification techniques (Jana et al. 2017; Luo et al. 2019; Borisyuk et al. 2018). It may be noted that, video subtitles is fairly common among videos downloaded from social media and thus, it plays a crucial role in event recognition. Oftentimes, unstructured video description present alongside online videos, may also be useful in video classification (Kalra et al. 2019).

1.2 Advances over the Years

Over the years, the researchers have resorted to various strategies and classification networks to predict the ongoing activity in video data. Initial advances involved maneuvering patterns only in the visual or auditory channel, where spatial information in the frames were made use of to arrive at a decision. On the other hand, some of the approaches preferred essentially image-processing oriented methods such as Scale Invariant Feature Transform (SIFT) (Lowe 2004), or Histogram of Oriented Gradients (HOG) (Dalal & Triggs, 2005) to localize features. The fact that temporal features, such as the ones that accounted for long-term motion patterns in the video frames were needed to better characterize the semantic aspects of a video, was later realized. Various classification frameworks involving convolutional neural networks were used, with variant architectures and varying degrees of precision. It was observed that deep networks performed much better when they were given an information about the precise spatio-temporal location of an on-going action. By virtue of temporal action-localization, the 'essential' temporal segments were fed to a classifier network which correspondingly categorizes each such clip. Some further improvement was achieved, by means of fusing the spatial and temporal (and in some cases, even auditory) streams to make the classification more robust. Predominantly early fusion, late fusion, Borda-count and other approaches were used in this regard. This also played a role in clearly discriminating the closely-related classes of actions in the videos. In Sect. 2, we provide a detailed survey of all these salient approaches and fusion techniques that have been adapted for the task of effective event classification.

1.3 Motivation and Our Contributions

Potential of Temporal Channel. As put forward by Girdhar and Ramanan (2017), c/activity recognition in videos as a simple classification of constituent RGB frames, even if they proffer good results in select datasets. To perceive how an object behaves with time, it is not only essential to pinpoint the spatial location of the 'same' object in every frame it is visible in, but it is also beneficial if its periphery of locomotion (to which it is restricted, over the whole time-span of the video) can be determined. Thus in our work, firstly we illustrate how holistically encouraging results can be obtained by choosing to exploit only the temporal motion patterns in videos, using a CNN-RNN hybrid model. Interestingly, in this endeavor, the results are found to be at par with some of the spatio-temporal approaches in use. Next, we record the improvement in event recognition accuracy when spatial information is combined with temporal ones. Essentially, we try to validate the fact that the temporal features, if exploited suitably, can solely prove to be useful for classification. This is due to their enhanced persistence through motion across the frames of a video.

Need for a Tailor-Made Fusion Strategy for Videos. We also venture on a less-trodden path of trying to effectively fuse the deductions from the spatial and temporal wings, while retaining their individual merits. Traditional techniques of early-fusion, suffer from being unable to exert much influence on the classification accuracy with respect to the diversity of multi-stream convolutional neural networks (CNNs). To state it otherwise, when parallel CNN streams deal with diverse modalities (as for instance, RGB and acoustic data), one may negatively affect the others' training phase. On the other hand, late-fusion generally performs better (Lee et al. 2018) in combining disparate multimodal information. However, video as a whole, bears a close relationship with its constituent frames—the frames' event should incrementally make up the video's event, even if there are minute dissimilitudes. Not all late-fusion strategies are effective in integrating this frame-to-video relationship. In contrast to such methods, we perform a multi-tier fusion, where fusion is performed on both frame-level and video-level predictions, in an attempt to efficiently integrate them. Here, the concept of *conflation* (Hill 2011) is used to consolidate two discrete probability distributions into a single representative distribution at every significant level of the strategy. This proves to be extremely useful in cases where a consensus between the streams is desired. A bias-factor is also specified for this conflation technique. This plays a key role in promoting the most confident prediction which both the streams are in agreement with on pertinent levels, as opposed to the general practice of favoring *any* one stream. This takes care of fine-grained intra-class variations as well. A class which would be otherwise wrongly predicted herein has the potential to undergo the various stages of our multimodal fusion strategy to be properly recognized in the long run.

It is especially encouraging to see the approach surpassing other multimodal fusion methods in use, on benchmark datasets such as UCF-101 (Soomro et al. 2012), Human Motion Database (HMDB) (Kuehne et al. 2011), Columbia Consumer Video (CCV) (Jiang et al. 2011), and Kodak Consumer Video (KCV) (Loui et al. 2007). Overall, our approach proves to be minimally demanding regarding the quality of capturing devices/camcorders, eventually giving rise to an efficient Cyber-Physical System.

1.4 Organization of the Chapter

In this chapter, we delve deep into the intricacies that concern the task of video surveillance at hand, through event classification and human-activity recognition, and discuss its various aspects thorough the segments of this chapter. The remainder of this chapter is organized as follows. In Sect. 2, we provide a detailed view of the various approaches that have played a key role in shaping solutions to automated understanding of events/activities. These include early approaches aiming to uncover structured patterns from motion, advent of space-time descriptor based methods and contemporary state-of-the-art solution frameworks relying upon deep neural networks. The development of various architectures and how they contributed in efforts to address the shortcomings of their predecessors over time is extensively highlighted. In Sect. 3, we broadly portray our approach to robustly perform video scene identification with a greater deal of precision. Section 4 accounts for the implementation aspects and records the results of the experiments conducted on four major benchmark datasets for event classification. Our solution framework is seen to provide a greater rise in precision on each stage of the multi-level feature-fusion strategy as compared to the state-of-the-art methods in use. Finally, we conclude and discuss the future scope of work in Sect. 5, with a note on the enhanced scalability of our solution, for use in Cyber-Physical Systems and understanding of events in video surveillance.

2 Related Work

Many Cyber-Physical Systems use smart computing techniques and remain embedded in larger physical systems e.g., a car, an aeroplane or a building to perform specific tasks. Very often, this CPS interacts with the surrounding physical environment through use of actuators and sensors. These embedded CPS devices communicate with some cloud backbone through communication networks to help taking subsequent decision quickly and promptly. Use of convolutional neural networks for possibility of a fire breakout (Saeed et al. 2019) and application of machine learning and its variants such as ensemble learning and instant learning (Alzubi et al. 2018), has shown interesting results. Application of unsupervised learning using K-Nearest Neighbours for human age recognition (Priyadarshni et al. 2019) is also significant. Text and face recognition from videos captured in public places (Jain et al. 2020) and facial emotion detection (Mukhopadhyay et al. 2020) provide interesting work in predicting potential criminal activities. Automated vehicle localization through space-time descriptor models (Sharma et al. 2019) and time synchronization in vehicular networks (Ghosh et al. 2011) are important milestones in traffic surveillance. In modern era, the advent of Internet of Things (IoT) have further revolutionized lives (Tanwar 2020). Several applications of IoT in different domains like, pharmaceutical fraternity (Singh et al. 2020) and healthcare in elderly patients (Padikkapparambil et al. 2020; Singh et al. 2020) have shown positive social impact. Bringing innovation to homes and common life, efficacy of IoT in household waste management (Dubey et al. 2020) and reliability analysis of wireless links for applications under shadow fading conditions (Sehgal et al. 2020) are worth mentioning. It thus may be pictured that the profoundly intertwined domains of computer vision and machine learning find heavy manifestation in fields of CPS and IoT, thereby changing everyday lives by leaps and bounds. With technological advances in a more demanding society, cyber crimes and threats of compromised security and privacy have become a concern too. The widespread popularity of hand-held devices including smartphones, laptops, palmtops is providing immense benefit of ubiquitous computing on the fly. However, this mass-scale computing also suffer from many cybersecurity challenges (Jana & Bandyopadhyay, 2013, 2015; Gupta et al., 2020) including phishing, IP masquerade attacks, denial-of-service attacks, mobile ad-hoc network security threats. Information security incurs major challenge when Cyber-Physical Systems avail cloud-based service, distributed throughout public domain of Internet (Ukil et al. 2013). Any Cyber-Physical System dealing with Internet of Things (IoT), exchange huge number of messages over Internet that requires a high-volume distributed file system to act seamlessly with reliable fault-tolerance (Paul et al. 2016). With these premises, we now proceed towards work on event and human-activity recognition in computer vision applied in video surveillance domain.

The problem of event recognition has garnered widespread interest in research in computer vision. The event recognition datasets that we work on, are replete with content diversity encompassing classes pertaining to domains. Examples include humanitarian basic action, outdoor scenes and indoor activities that may even occasionally feature various animals in action. This motivates us to provide a backdrop for discussion of the various approaches that researches have resorted to over the years. In subsequent sections, we highlight many of these significant approaches across time.

2.1 Early Concepts of "Structure from Motion"

One of the earliest and most intriguing works were by Potter (1976) in the year 1976, which being a paper in transcendental psychology, presented assessments of the human mind's ability to retain information about a series of pictures flashed in a rapid sequence. Evidently, the *gist of a video*, or what may be called a brief understanding of complex content was being studied. Speculations are that, this planted the seeds of interest in the then newly conceived discipline of computer vision, whereupon the aim was to automate the understanding of these events or in essence, high-level complex activities. In the early 1990s, methods were being developed to tackle the very basics, the smallest of gestures, for instance "the raising or moving of a hand". Analysis of the body posture featured as a recurrent theme in many of these works. Psychological studies once again lit the scenario up, as the works of Johansson showed that gait analysis and motion could be tracked through Moving Light Displays (MLD), that were not in the least affected by external distractive features such as the lack of illumination in the video scene, or jitter, semantic spatial background variation. For instance, an MLD would specifically not distinguish between a man jumping in a forest and a man jumping on an asphalt road, since the motion is all that bears emphasis for an MLD system, which is in this case of course, jumping. Some of the contemporary approaches to tackle the problem in the field of computer vision, wound around the aim of automated interpretation of MLD results. As discussed in the works of Cedras and Shah (1995), quite a few of the works were found to be based on the concept of efforts to quantify Structure From Motion (SFM). SFM relied on exploiting the three-dimensional coordinates of all the objects in motion in the input video that would reveal some information about the way they execute their motion. One of the frontiers that accelerated the progress in this regime was *optical-flow*. A method that made computational sense of the pattern of motion of the objects, depending on the way their movement changed across successive frames in a video, optical-flow has stood the test of time, still a go-to resort for many enthusiasts in the field. The fact that it also accounts for the change of the object movements with sustainable camera movement, makes it an effective SFM method for articulating motion over time. Mathematically, an optical-flow vector could be interpreted as a two-dimensional vector field with each entry signifying the displacement of the particular point in consideration from one frame to the successive one. The method is powerful in the sense that it provides considerable information about the velocity of movement, and the part of the frame featuring the said object. As an immediate corollary, it found its practice and use in the domain of surveillance and effective tracking of vehicular motion. This paved the way for many more advances in the allied fields of object tracking. Many standard methods are in vogue for computation of optical-flow, some of the most prominent being the works of Horn and Schunck (1993), and Oron et al. (2014), being predated by the traditional methods of block-based and phase-correlation methods.

A number of methods followed the advent of the optical-flow algorithm, which were trajectory-based. This served as a ground for computational realization of relative motion of objects in a single video frame. It served as a citation of the potential power of temporal features, which until then had often either been a moot-point or viewed as a mere auxiliary of the spatial information a video had to offer. Accuracy is at times, seen to fluctuate, for methods based on optical-flow are prone to be affected by low illumination, cluttered background and instances of occlusion present in the videos. Clarity is sought primarily in a number of approaches, where ambiguity is to be eradicated in the discovered trajectory points. Even then, it serves as one of the most prominent means of accounting for the temporal features that have a telling effect on recognizing the activity in the video. At this juncture, Elgammal et al. (2000) suggested segregation of images into two salient parts, namely the background and the foreground, could turn out to be useful in tackling the problem of recognizing events. To reinforce the conceived idea, instances of identifying the human body structure from silhouette-images or frames. Thus, background subtraction to focus on the entity in the image executing motion was of interest. The silhouettes in turn, can be uncovered using now renowned algorithms such as the Grab Cut algorithm proposed by Rother et al. (2004) that can separate the foreground object from the ambient background. The contour of the foreground object involved in the activity can thus be analyzed in this approach, thereby helping one to assess the impact of considering the size, shape and pattern to realize the. The extracted silhouettes can serve as useful information, emphatically so when human activities are involved, so that the gait patterns may be studied. It was at this time that a pioneering work by Polana and Nelson (1994) dealt with non-parametric approaches for machine perception of activities. Before moving on to the discussion of the various three-dimensional, local-descriptor based methods to quantify actions, it is worth mentioning the two-dimensional formulations the authors came up with. Motion was first articulated through temporal difference images, and Human presence was detected through the study of both either extracted silhouettes, as well as from a *trajectory primal sketch* obtained from the MLD applications, inspired by the works of Gould and Shah (1989). "Action" was an entity that they classified into two main kinds—*stationary* and *non-stationary*, owing to the fact that stationary events such as sitting would not cause significant geometric translation of the person executing the motion, as compared to non-stationary ones such as walking, running, playing and so on. Actions of different kinds relevant to the dataset are marked with varying levels of periodicity by the nature in which they are executed, whereupon periodicity in the action video is detected using Fourier Theory. According to the concept, actions found to be considerably periodic are detected by this approach. An impressive account which builds on this concept is presented by Bobick and Davis (2001), in which the activities and the fine transitions between them are given increasing importance, and first individually mapped onto a representation the users call a *temporal template*. The temporal templates across the length of frames are then aggregated effectively to express the action, in its making. On giving equal weight to each of these constituent frames, we are led to the representation of the *Motion Energy Image* (MEI) template. While a MEI can traditionally stand for the intensity of the activity, on the other hand another informative portrayal is found in the *Motion History Image* (MHI) where one can get an idea to how exactly the particular motion was executed over time. As an example, it could map the sequential forearm movements of a tennis player distinctly depending on the kind of shots he/she chooses to play. These templates prove to be one of the most prominent amongst the early advances of tackling the problem of event and action understanding significantly in video data, and form the basis for further enhanced studies on the same.

2.2 Space–Time Descriptors

The progress of understanding high level activities in video content, took a rise with proper interpretations of *features*, which could now venture along space and time fields. The *Harris Corner Detector* in its two-dimensional form, was used to demarcate spatial points in an image, with a degree of content intensity variation above a certain threshold, as discussed in the work by Derpanis (2004). A powerful extension was provided in the renowned work by Laptev (2005), in which a three-dimensional extension of the basic Harris Corner Detector was proposed. The inclusion of a third dimension accounted for the fact that now temporal relevance would be highly recognized as a factor for recording regions of change in the frame image. A fresh concept of "Space-Time" or "Spatio-Temporal" Interest Points (STIP) was obtained through this perspective, and these interest points were profoundly insightful to exploit since they carried the spatial content information, as well as ensured the temporal relevance of the motion pattern that sustained the content change. A beautiful illustration that could help us better comprehend the phenomenon could be through an example, as in Fig. 2.

The intriguing fact worth mentioning in this approach that the points where temporal movement is considered noteworthy, across the length of the frames for the video, instead of just accounting for spatial changes such as appearance of a new object in the scene (which in this case, may be thought to be the ball). The first frame where the ball enters the scene, causing content change does not locate it as a potential spatio-temporal interest point just then, because it does not contribute any change to the location of the region in which it appears in the image. Across the frames, the batsman does not let his head stance position vary too much, which evades it from being a strong point of interest, and gets shadowed by other points in

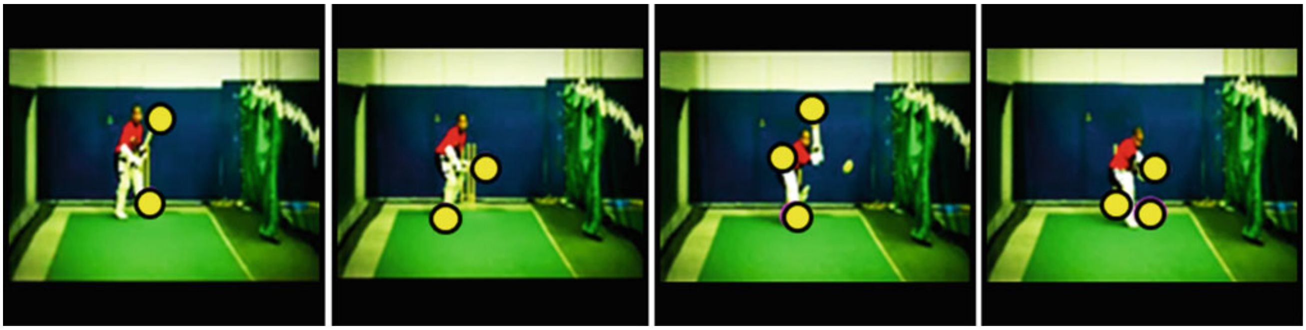


Fig. 2 An illustration of how *Spatio-Temporal Interest Points* (marked in yellow circles) obtained through the extended 3D Harris Corner Detector could be key to comprehending actions manifested across frames across video (in selection: 'Cricket Shot' from UCF-101 Soomro et al. (2012) dataset)

its vicinity. These points evidently undergo a comparatively effective displacement in the dimensions with respect to the boundary points, in the extended formulation of the Harris Corner Detector. These are the points which execute motion significant enough to portray the characteristics of the action class (in this case, Cricket Shot). Thus, although the portion of the image containing the entrant ball is not initially labeled "a point of interest", it gets included in afterwards, when the ball is hit by the batsman, explicitly indicating the motion of the cricket shot being played.

Based on this extension, Blank et al. (2005) devised a novel strategy to not only mark the points of action, but also to model the activity in transit. For instance, the motivation here was to discover what kind of a spatio-temporal volume could imply a particular action class. At this juncture, one might rightfully draw a few parallels with the work of Polana and Nelson (1994), whereupon the authors interpreted actions to be periodic. The merit here, with mathematically articulating the way an action evolves over time, one is able to eradicate the over-dependence on periodicity, and is able to recognize it instant whenever it is a trait of the particular activity class. Limb movements in walking, or repeated structure of motion patterns as seen in cycling, might serve as particularly relevant examples. Once visualized geometrically, the scenario translates into the idea of a spatio-temporal cuboid. This maps the degree of movement seen in the video through representative blocks sampled over parameters (space, time and volume scales). In a work by Wang et al. (2009), the efficacy of these important points-of-interest are elevated by trying to extrapolate the Hessian detector to a third dimensional strategy, in a manner akin to the Harris detector. It is seen in hindsight, that these cuboids, serving as local descriptors may be used to map some motion trajectories from which motion that exerts dominating effect on classification of its kind or scene understanding, can be uncovered. However with unconstrained videos, shot with lack of proper professionalism, there may be occasionally jittery content, and the dexterity of the local descriptor approach is found to be debatable in such cases. There might be relative motion in the actions, and there might be camera-movement in the video sequences as well, leading to motion depth considerations studied in considerable detail by Jiang et al. (2012). This also paves the way for a discussion of the more recent approaches to the problem of event recognition in unconstrained video data, many of which make use of deep neural network architectures in various forms.

2.3 Recent Approaches Using Deep Neural Architectures

Having adopted many strategies based on mapped templates, hand-crafted features, and local descriptors over a span of a decade or more, the research community felt the urge to try using deep learning models for a better understanding of the unconstrained video scene. Convolutional Neural Networks (CNNs) proved to be stunning in their work of classifying images, as various architectures of CNNs continued to ace the Imagenet Classification Challenge Russakovsky et al. (2015), each subsequent neural network model appearing to be more proficient in the task of classification than its predecessor. This excellence of CNNs in general while dealing with image content, served as further motivation to deploy them in the task of video recognition. Another inclination which contributed to the rise of deep learning models in the solution of this problem was the fact that hand-crafted features, when learnt, were often found to be reliant on the video quality in general. These also fell short in accounting for the widespread content diversity of classes that the activities or events occurring in the videos. This was observed to be true in the case even where these individual features were aggregated through a dictionary-based codebook or vocabulary of visual features, that attempted to extensively markdown some distinguishing action patterns for each of the applicable classes. The approach was named the *Bag of Visual Words* (BoV), and efforts to strengthen it were made by making the features being aggregated powerful, with techniques such as *Histogram of Gradient*s (HoG) and *Vector of Locally Aggregated Descriptors* (VLAD) being used. Although temporal relevance was given some attention, in a modified approach, it called for more significant importance, due to the sheer amount of enormous possibilities and diverse semantic characterization that each of the activity classes could potentially bear in a dataset.

Some of the initial CNN networks, intuitively exploited the spatial features that the videos contained, as the models were fed with successive frames of the video. Alternatively, this was also effectuated by performing image classification and/or semantic segmentation Mukherjee et al. (2020) on the individual frames. Such spatial techniques can correlate a scene's subject to the background, thereby realizing the scene content; as for instance, the common appearances of a soccer ball in a stadium or gallery, and the fact that a football match could be prevalent in the event. Intriguingly, this instance could lead one to dawn upon the fact that the spatial features alone could often be misleading for the task of classifying scenes. An intuitive example, would be the fact that the spatial information "stadium" or "green grassy fields" could relate to more than just one class of events, such as "soccer", "cricket", "baseball", or for that matter any generic outdoor sport activity. So, spatial CNNs were in vogue across various architectures, until the growing importance of temporal features were something that could no longer be avoided. Temporal features would directly correlate with the limb movements and other respective motion patterns, associated with the particular action. There could be ways of exploiting this through SFM methods that we discuss in the earlier section of approaches. The processed image data obtained as a result of the applied SFM technique can be then fed as input to the CNN model. In their work, Zhang and Xiang (2020) make use of SIFT, HOG and *local binary patterns* (lbp) to localize the temporal information, that is the persons in the image executing the action. A temporal CNN could be designed across a variety of CNN architectures. Some authors while studying temporal features resort to Recurrent Neural Network (RNN) architectures. As the name suggests, they are capable of accurately picking up long term motion implications and specific pattern sequences that correlate to some classes. The fact that these recurrent architectures have various memory cell units integrated that help them to retain sustainable information, and a feedback layer which ensures the learning is robust across time samples to account for the entire length of the data. Approaches relying exclusively on temporal features for video classification are substantially less, and we (Jana et al. 2019) in one of our works, demonstrate the immense potential they have as sole performers itself, till an extent where we show them to be not only capable of outperforming standard exclusively temporal methods, but also being at par with some of the spatio-temporal techniques of classification. This is because of the hybrid deep learning model that we use. Choosing a set of representative key-frames that represent the video content for each class with minimized temporal redundancy, we perform optical-flow on these selected key-frames. To localize the robustly significant actions that characterize the activities, we feed the magnitude images of these optical-flow images to our deep learning framework, which comprises of a CNN-RNN (LSTM) fusion. This signifies the fact that the output predictions of the CNN model serves as input vector, duly reshaped for the RNN framework. At this juncture, it is worth mentioning that we use the ResNet-50 architecture as the CNN, which being a residual neural network exploits action features considerably from the input magnitude images, being considerably "deeper" than the likes of VGG and Inception-Net that shortly precede the advent of strong residual blocks in a deep neural network. This speaks for the fact that a CNN-LSTM fusion for temporal features proves to be more than dexterous in the task of classifying videos into action classes.

However intensely dedicated these networks might be for the task of recognizing exclusively spatial or only temporal features from a video in order to furnish optimized classification results, it was realized that the two indeed had to go hand in hand. Thus rose the concept of multimodal deep fusion techniques, that contributed to a lot of interesting studies and some really notable advance in terms of identifying action classes from disperse datasets. Various methods of multimodal fusion are some of the foremost approaches that yield truly encouraging results in comparison to the standard uni-stream ones. The authors exploit parameters across three main streams (visual, action and auditory stream) in an intriguing approach of "Who", "What", and "Where", in an effort to characterize the scene content (Zhang & Xiang, 2020). The deep learning framework they come up with is a multi-stream CNN with features being globally pooled across the respective frameworks, to give multimodal cues.

Figure 3 articulately demonstrates the need for a "spatio-temporal" fusion approach in solving or designing a deep neural network in order to learn the characteristics of the various activity classes in the datasets. It is interesting to see how the frames of videos essentially belonging to centrally similar theme (kicking/soccer) but evidently they are distinct classes, as it can be seen. This speaks for itself why exclusive spatial information such as a lush green field, stadium, or even sole temporal features such as foreword limb movement for the task of kicking are not sufficient to accurately classify the event since "Soccer Juggling" would have minutely different motion intensity pattern than that of a "Kicking" class, which might be done in any kind of an ambiance and not necessarily on a field. 3-D Convolutional Neural Networks are statistically seen to outperform their two-dimensional counterparts, due to three dimensional kernels, which helps extract features corresponding to a third axis, denoting time. A host of approaches present score and rank-level fusion, often on accuracy values obtained on separate streams of the multimodal network, but this quite naturally leaves behind a semantic gap to be bridged. On the other hand, some of the approaches by Luo et al. (2019), and Li et al. (2020) attempt to exploit the spatio-temporal features through fusion of the respective softmax scores of the deep learning model. Another set of salient approaches perform weighted conglomeration of the extracted features from each of the representative multimodal streams, be it visual, motion or auditory, in a secondary max-pooling layer of the network, with an intention of thereby promoting the best of those extracted across each wing, as is the motivation seen in Cherian and Gould (2019). The reason these models sometimes fail to offer the precise classification result for an event class, is due to the underlying ambiguity of the *degree of importance* that features uncovered from a particular stream or wing deserves, for instance the auditory features extracted in a particular case might be promoted largely due to its intensity despite the fact that it is misleading and could have might as well be suppressed.

An interesting study of the concept of *coherence*, that gives an assertive suggestion on when one may opt to suppress the temporal stream and focus on the exploitation of the spatial wing is due to the Siamese Network, conceived by Lu et al. (2017). As shown parallely in the works of Varior et al. (2016), Siamese Networks have the ability to take entire video sequences as input and decide on whether the temporal variation in the frames is significant enough to be given an enhanced priority over the visual stream, or vice-versa. To eradicate such possible anomalies comprehensively, during fusion we (Jana et al. 2019) resort to a multi-tier conflation based strategy that provides us with a noteworthy increase in the number of correct classifications, as we achieve the con-

(a) Soccer Juggling

(b) Soccer Penalty

(c) Kicking Ball

Fig. 3 Illustrating the need of a *spatio-temporal fusion network* rather than an exclusive one, to accurately identify event classes, related to a central theme (in this case, kicking/soccer)

sensus from both video and frame levels. Closely related to the concept of spatio-temporal fusion, an illuminating work on the domain by Karpathy et al. (2014), while working with the UCF-Sports dataset, deals with a concept of fusion coupled with a foveated architecture. Apart from spatio-temporal streams, the deep learning CNN model is equipped with a "*fovea*" stream, which stands for *central view*. The fovea stream contains a central crop of the frame image of the input video, somewhat akin to a *zoom-in* effect. It plays the role of substantial auxiliary information that guides the CNN with some added details that prove crucial to characterize the event, as we show in Fig. 4. This was seen to improve recognition results. However it is quite intuitive that the interpretation of the foveated image as a centrally cropped image from the main frame is better suitable for sports classes in general, than for generic event identification. The puzzle of having a competent enough fovea stream for a broader spectrum of events is a problem that is being currently worked upon, as the concept of an added "attention" to what is usually at offer across the multimodal streams, is believed to be able to boost the classification results by a considerable margin. This can undoubtedly have a telling effect on many areas of Cyber-Physical Systems and surveillance, since it helps in pinpointing the action of important interest, and thereby tracking it with a greater degree of precision.

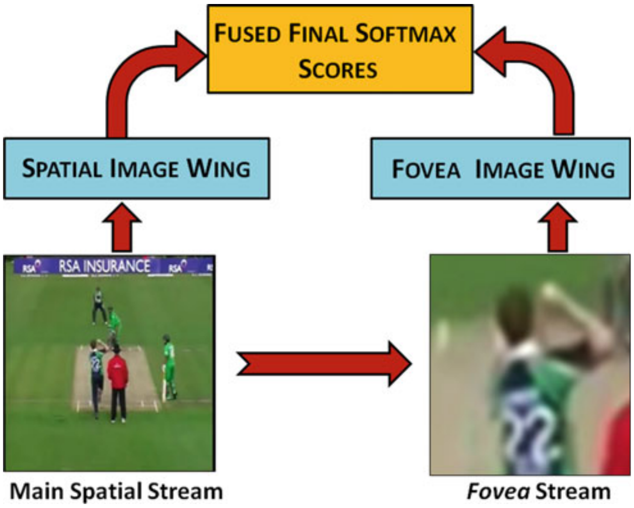


Fig. 4 Deep architecture with *fovea* stream by Karpathy et al. (2014)

3 Video Scene Identification

We start our event-recognition pipeline with reduction of the space of frames. This is done by a systematized key-frame selection technique (Sect. 3.1). Firstly temporal redundancy is reduced by eliminating redundant information. Then the most distinctive set of frames are chosen by a graph-based approach. These form a representative set of frames for the video. This is followed by extracting multimodal information from those key-frames (Sect. 3.2). Next, these multimodal features are maneuvered through separate dedicated deep architectures. Finally, the respective frame-level and video-level predictions are fused (Sect. 3.3) from each such modality channel, to proffer a final decision pertaining to a video.

3.1 Key-Frame Sampling

In all videos, the physical setting or the backdrop remains constant throughout majority of the duration. But, there are specific time-spans of the video when the scene changes, either gently (*gradual transition*) or in suddenness (*abrupt transition*). As such, the whole time-duration of a video can be broken down into a number of semantically-meaningful fundamental structural units, known as *shots* (Mohanta et al. 2011). These can be regarded as a set of frames, that appear at successive time-stamps and have similar spatial appearance, when the video is played. Now to obtain a *storyboard* from a video, it is essential to retrieve one/more representative frame(s) from each such shot. These are collectively known as *key-frames*. The better the set of key-frames chosen, more is their viability to be regarded as a summary of the whole video.

Upon more deliberate thoughts on the underlying concept behind representative frames, another inherent property becomes apparent. The number of key-frames chosen from a fixed time-span should be directly proportional to the number of key-frames chosen from that span. As for example, let's suppose that the frames of a sixty second video practically shows no considerable motion during the first fifty seconds, and all the actions are packed in the last ten seconds. In this case, most of the key-frames should ideally be chosen from the last ten seconds (even though its span is smaller), and a handful from the first fifty seconds. We follow a two-stage process (Jana et al. 2019) to sample a set of n_{KF} key-frames from a video, as explained in the subsequent paragraphs.

Reduction of Temporal Redundancy. As we understand, frame-sampling should be from the temporal (time) axis. Firstly, we reduce the temporal redundancy by replacing the *similar* (with respect to motion of constituent pixels) frames, by a single representative frame. This is started off by computing the dense optical-flow (by any classical algorithm such as, Horn–Schunck (1993) or Lucas–Kanade (2014) between consecutive pair of frames. Thereby with each pixel (x, y, k), a flow-vector $(u\delta k, v\delta k)$ is associated that corresponds to its spatio-temporal displacement to a new location, $(x + u\delta k, y + v\delta k, k + \delta k)$. For consecutive frames, $\delta k = 1$ and thus, we can represent the magnitude and slope of flow-vector as, $\sqrt{u^2 + v^2}$ and $\tan^{-1}(\frac{v}{u})$ respectively. Further for a frame, the overall distribution of motion can be quantified by histograms of magnitudes and slopes of corresponding flow-vectors of constituent pixels. These two histograms are then concatenated, to represent a frame's motion (henceforth called as *motion-histogram*, by us). The next task is to determine if consecutive frames are homogeneous with respect to motion. If that is the case, we may not take both but discard one of them. We, therefore, record the temporal disparity ($\text{td}_{k\to k+1}$) between successive pair of frames, $I(:, :, k)$ and $I(:, :, k + 1)$, as the ℓ_1-norm of corresponding motion-histograms. When this temporal disparity ($\text{td}_{k\to k+1}$) is less than a certain threshold, it can be adjudged that the corresponding frames are *temporally redundant*—thus, one of them is discarded. An optimal value of the minimum threshold (td_{min}) is statistically found to be

$$\text{td}_{\min} = \overline{\text{td}} - \hat{\sigma}_{\text{td}} \tag{1}$$

where, $\overline{\text{td}} = \dfrac{1}{N-1} \displaystyle\sum_{i=1}^{N-1} \text{td}_{i\to i+1}$ and $\hat{\sigma}^2_{\text{td}} = \dfrac{1}{(N-1)-1} \displaystyle\sum_{i=1}^{N-1} (\text{td}_{i\to i+1} - \overline{\text{td}})^2$. At the end of this step, we get a subset of frames from the video that are temporally distinct w.r.t. associated motion of pixels. The search-space of key-frames is thus drastically reduced, making our subsequent step computationally efficient and effective.

Selection of Distinctive Frames. This stage begins with the subset (S) comprising of temporally distinct frames, from the previous step. Firstly, a *complete graph* is formed each of whose vertex corresponds to a frame from S. For any two vertices (frames) v_i and v_j, the weight of the edge connecting them is the temporal disparity $\text{td}_{i\to j}$, i.e. the ℓ_1-norm of corresponding motion-histograms. Thus, the edge-weight can be physically interpreted as the temporal (w.r.t. motion of constituent pixels) distinctiveness between frames—edge-weight increases with disparities in flow-vectors.

But, maximizing distinctiveness amongst frames is not sufficient for an effective key-frame selection algorithm. Let us consider the example yet again, that we gave in the introductory paragraphs of this section—a 60 s video, with no considerable motion during the first 50 s, and all the actions packed throughout the last 10 s. Since all our frames in the last 10 s change most rapidly, an algorithm solely reliant upon temporal distinctiveness would be biased to choose frames that are in close time-proximity to one another (within the last 10 s).

Thus, our motive of story-boarding the whole video will not be satisfied here if we rely only upon temporal distinctiveness. To solve this problem, we store the timestamp of each frame corresponding to the node it represents in the complete graph. And in each iteration while choosing the most distant (distinctive) pair of nodes (frames), we pay a close attention to these timestamp values to decide upon whether to include the edge they represent, or not. This condition is regarded as the '*viability*' of the edge. An edge can be chosen in a particular iteration if and only if it is viable, and moreover, edges once marked as non-viable are not considered for inclusion in any of the further iterations. For an edge to be considered as *viable* for inclusion, two conditions must be satisfied:

- Difference in timestamps between terminal nodes of the edge should be above d_{low}.
- Difference in timestamps between each of the terminal nodes of the edge and any previously chosen node, should be above d_{low}.

Here, d_{low} is the minimum acceptable time-gap between any two chosen key-frames and its value is $\left\lceil \frac{N}{2 \times n_{\text{KF}} - 1} \right\rceil$. As we defined in our introductory paragraphs, n_{KF} is the preset and fixed number of key-frames, we want to represent a video by. This value arises after allowing a relaxation on the stringent time-gap of $\left\lfloor \frac{N}{n_{\text{KF}} - 1} \right\rfloor$, that must be satisfied when we want the frames to be equally spaced across the time-axis.

In this way, frames are selected from the graph until $\frac{n_{\text{KF}}}{2}$ iterations are completed, or all edges are marked as un-'viable', whichever occurs first. In each iteration, one edge i.e. two vertices are selected.

This stage is explained pictorially in Fig. 5. We consider a video consisting of 2195 frames, in total. Supposing that only ten frames were obtained in subset (S) (comprising of temporally distinct frames) from the first stage, a complete graph of ten vertices were formed initially. Also, considering that we require $n_{\text{KF}} = 6$ key-frames to be chosen from the video, there would be a maximum of $\frac{n_{\text{KF}}}{2} = 3$ iterations. Thereby, in this case, the minimum acceptable time-gap (d_{low}) between any two chosen key-frames takes the value of $\left\lceil \frac{N}{2 \times n_{\text{KF}} - 1} \right\rceil = \left\lceil \frac{2195}{2 \times 6 - 1} \right\rceil = 200$. For each iteration, all the 'viable' edges are shown as *black solid lines* in Fig. 5. Further, the most distant pair of vertices from amongst the viable edges are shown by a *superimposed red dotted line*. Terminal vertices of already chosen edges are shown to be *ticked*. At the end of three iterations, the chosen edges are (0, 5), (4, 7) and (2, 3), in order. The six key-frames chosen through the three iterations, are displayed again at the bottom with their respective timestamps. It is evident that the time-span $t = 455$ to $t = 1443$ is more action-packed than $t = 1444$ to $t = 2195$, because more key-frames were chosen from the former.

3.2 Realization of Spatio-Temporal Features

Two types of features are focussed on, in the current work viz., *spatial* and *temporal*. Moreover, we are only interested in the features extracted from the key-frames. The spatial feature is associated with the space of a single frame. It is realized by the raw RGB-image form of a key-frame. On the other hand, the temporal feature is associated with the transition from one frame to another. To retrieve the temporal feature from a frame $I(:, :, k)$, the dense optical-flow (by any classical algorithm such as, Horn–Schunck (1993) or Lucas–Kanade (2014) is calculated between $I(:, :, k)$ and its immediate next frame, $I(:, :, k+1)$. The temporal feature is represented by the grayscale image where each pixel position (x, y) gets the magnitude of the flow-vectors at $I(x, y, k \rightarrow k+1)$. The magnitude value is normalized in the range [0, 255].

3.3 Deep Neural Architecture and Decision-Fusion

After extracting multimodal information (here, spatial and temporal), there is a need to combine these such as to get a single probability distribution (for logistic regression) or, a single prediction class pertaining to a video. Keeping deep learning based classification approaches in mind, broadly, the fusion (Liu et al. 2018) strategies can be classified under the following subheadings:

- ***Feature-Level Fusion***. This is also known as *early fusion* or *data fusion*. It creates a combined feature-vector representation by *concatenating* all the input feature vectors, corresponding to each of the modalities. Subsequently, this combined feature-vector is trained on a single classifier model. The classifier model must be compatible to tackle all the modalities simultaneously. Moreover, this necessitates the combined vector to be pre-processed separately and aptly, such that it is suitable for the single classifier model.
- ***Kernel-Level Fusion***. Here, the fusion operation is closely interleaved with the training of classifier. Kernel function is a mapping, that is applied on a set of non-linearly-separable data-points to map them to a higher dimensional space (such that now, they gets linearly separable by a hyperplane). As such, they enables a linear classifier to be applicable towards linearly-inseparable data-points. In this fusion strategy, corresponding to the feature sets from each modality, the kernel-values are calculated separately each time. After this, they are integrated to form a new composite kernel-function.
- ***Decision-Level Fusion***. This is also known as *late fusion*. It combines the unimodal predictions (class label/probability distribution) from the last fully-

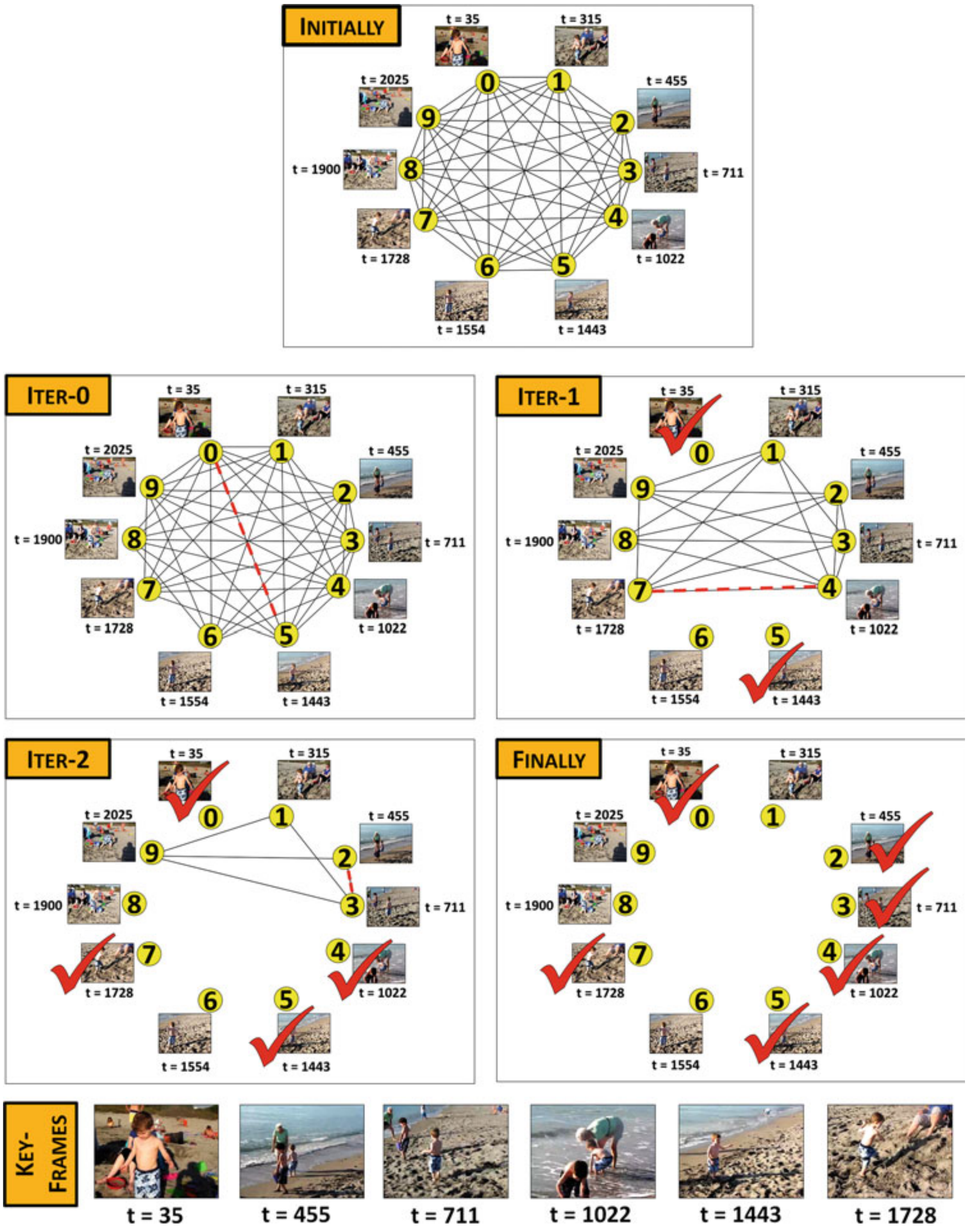


Fig. 5 Demonstration of the stage of "Distinctive Frame Selection" subsequent to reduction of temporal redundancy. The chosen key-frames are displayed at the bottom with their respective timestamps of appearance

connected layer of each single-frame classifier stream (each relied upon for different modalities) of an ensemble network. Since this is used to consolidate scores *post-classification*, researchers (Rana 2011; Pinar et al. 2016) are of the opinion that the raw-data level correlations are not properly exploited. Nevertheless, this allows to have a separate classifier model, each well-suited to tackle each modality.

Regarding the deep neural architecture, we employ a hybrid architecture (Jana et al. 2019), comprising of a Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN). While the CNN portion is manifested by ResNet50 model, we use a LSTM network to realize the RNN counterpart. The flow of data through this hybrid model goes like this: (i) A certain modality information (spatial or temporal) is exploited from each of the key-frames pertaining to a video, and fed to the CNN (ii) Corresponding to that particular modality (spatial or temporal) for each key-frame, the CNN provides us with a prediction vector at the last fully-connected layer and one/more feature vectors from the preceding fully-connected layer(s). The prediction is in the form of a L-class probability distribution, where the lth value represents the probability of that frame to belong to the lth category/class. These are henceforth regarded as *frame-level predictions*. (iii) Next, the frame-level features of all the key-frames pertaining to a video are accumulated. They are reshaped appropriately to three-dimension before being fed to an LSTM network. (iv)

The LSTM, in turn, outputs a single probability distribution for a video that ideally acknowledges prediction of each of its constituent key-frame. This prediction is also in the form of a L-class probability distribution. But in contrast to the frame-wise prediction, the lth value represents the probability of the whole video to belong to the lth category/class. Thus, we refer this as a *video-level prediction*.

Next concern is to consolidate all the frame-level probability distributions of constituent key-frames and the video-level prediction, for each modality. Most researchers (Wu et al., 2015; Peng et al., 2017; Cherian & Gould, 2019) prefer to use average of probability distributions, to integrate them. But, it does not always provide a desirable solution. This is because the consolidated distribution can give a completely new distribution, that is consistent with none of the initial distributions. So, we prefer to use a *biased conflation* (Jana et al. 2019) of probability distributions. Moreover, making the whole process multi-tier gives us a systematic approach that integrates frame-level and video-level predictions effectively.

Biased-Conflation. For two probability distributions P_1 and P_2, their conflation is defined as,

$$P_{\text{conflated}}(X = a) = \frac{P_1(X = a) \times P_2(X = a)}{\sum_{b=1}^{X_{max}} P_1(X = b) \times P_2(X = b)} \quad (2)$$

To this, we adopt a biasing technique to make it close to reality (i.e., one of the initial distributions). The Bhattacharyya distance (Bhattacharyya 1946) from $P_{\text{conflated}}$ to P_1 and from $P_{\text{conflated}}$ to P_2 are computed. Thereafter, the conflated distribution from $P_{\text{conflated}}$ is biased to the closer distribution (from amongst P_1 and P_2) with an appropriate biasing factor, dependent on these two distances.

Cross-Fusion and Self-Fusion. Apart from the concept of biased-conflation, we introduce two types of fusion. *Cross-Fusion* is defined as the biased-conflation of probability distributions, belonging to two different modalities. *Self-Fusion* is defined as the biased-conflation of the probability distributions, corresponding to all the key-frames of a video. We go on aggregating distributions in a hierarchical and multi-tier scheme (Jana et al. 2019). Effectively, cross-fusion of frame-level (or, video-level) distributions give similar frame-level (or, video-level) distribution. On the contrary, self-fusion of frame-level distributions return video-level distributions. So, cross-fusions are applied in the same hierarchy, while self-fusion is applied to move up the hierarchy ladder.

4 Experimental Results and Discussion

As we stated previously, an efficient Cyber-Physical System (CPS) intended towards video surveillance, depends heavily on the capability of its backend algorithm. To state it otherwise, this algorithm should be equally proficient towards scene understanding or event classification on one hand, and human activity recognition, on the other. Moreover, since video capturing devices are often inexpensive, the recorded videos suffer from serious quality issues. Thus to acknowledge how the proposed method fares towards these surveillance systems, we evaluate our results on the following datasets:

(i) **Columbia Consumer Videos (CCV)** (Jiang et al. 2011): This dataset is consisted of 9317 unedited consumer videos from YouTube, that can be sub-classified into 20 event categories. In this collection, low-level events like, locomotive objects (“bird”, “cat”) and outdoor scenes (“beach”, “playground”) coexist side-by-side with high-level events like, sports (“biking”, “ice-skating”), and social gatherings (“parade, “birthday”).
(ii) **Kodak Consumer Videos (KCV)** (Loui et al. 2007): This dataset includes 1358 quality-degraded videos from the actual consumers of Eastman Kodak Company’s products, and 1873 videos from YouTube. These videos are spread over the broad categories of activities, occasions, scene, object, people and sound, that accounts for a total of 29 event-concepts.
(iii) **UCF-101** (Soomro et al. 2012): This dataset includes 13,320 short clips from YouTube distributed across 101 action classes. Although the videos does not go beyond realistic human-action, the diversity in actions ranging from small-scale facial movements to large-scale locomotory activities, is what makes this dataset challenging.
(iv) **Human Motion Database (HMDB-51)** (Kuehne et al. 2011): This has 7000 clips spread over 51 human-action categories, collected from numerous freely-available movies on Prelinger archive, Google and YouTube. Videos showcase quality aspects, characteristic variance in duration and have stabilization issues.

While the first two datasets deal with unconstrained videos and event classification, the latter two are focused on human-activity recognition. Thereby, we aim to provide a exhaustive performance evaluation of our method.

We have based our evaluation in two stages. We told in our motivation (Sect. 1.3) that we intend to show the potential of a standalone temporal stream. The first stage evaluation is based upon this idea. With this in mind, in Table 1, we tabulate some of the past and recent state-of-the-art (SoTA) methods that focussed exclusively on temporal feature. With these methods, we compare the performance of our temporal CNN-LSTM stream. Although our method surpasses all the tabulated SoTA methods in event recognition on CCV and KCV datasets, there are still scopes of improvement in the temporal-based human-activity classification on UCF-101 and HMDB-51 datasets.

Table 1 Performance comparison of different approaches employing temporal features exclusively, on each of the four datasets

Dataset	Method	Description	Acc (%)
CCV (Jiang et al. 2011)	Wu et al. (2015)	Temporal LSTM	54.70
	Wu et al. (2015)	Temporal ConvNet	59.10
	Li et al. (2020)	Temporal ResNet + hierarchical attentions	63.62
	Zhang and Xiang (2020)	Temporal LSTM to *fc8* of VGG-19	63.80
	Ours (Jana et al. 2019)	**Temporal action localization, CNN + LSTM**	**79.13**
KCV (Loui et al. 2007)	Duan et al. (2012)	SIFT features	35.46
	Chen et al. (2013)	Space-time features + MDA-HS	49.61
	Luo et al. (2018)	Semi-supervised feature analysis	47.70
	Ours (Jana et al. 2019)	**Temporal action localization, CNN+LSTM**	**52.41**
UCF-101 (Soomro et al. 2012)	Wu et al. (2015)	Temporal LSTM	76.60
	Wu et al. (2015)	Temporal ConvNet	78.30
	Wang et al. (2016)	ConvNets (Optical-flow + warped flow)	87.80
	Mazari and Sahbi (2019)	Temporal pyramid + multiple representation	68.58
	Peng et al. (2017)	Temporal stream of 2-network VGG-19	78.22
	Zang et al. (2018)	Temporal-weighted CNN + attention	88.30
	Zhang and Xiang (2020)	Temporal GRU to *fc8* of VGG-19	64.50
	Ours (Jana et al. 2019)	**Key-frame, temporal CNN + LSTM**	**66.57**
HMDB-51 (Kuehne et al. 2011)	Girdhar et al. (2017)	ActionVLAD flow-stream	59.10
	Cherian and Gould (2019)	ResNet-152 (Frame-level SMAID + Opt-Flow)	59.50
	Zhang and Xiang (2020)	Temporal LSTM to *fc8* of VGG-19	33.30
	Li et al. (2020)	Temporal ResNet + hierarchical attentions	37.29
	Ours (Jana et al. 2019)	**Temporal action localization, CNN + LSTM**	**55.67**

Evaluation is made based on average accuracy (Acc) over all classes, expressed in percentage

The second stage evaluation is based upon improving this deficiency, with an efficient multimodality fusion strategy. We made this experiment with only two multimodalities viz., spatial and temporal. But this can be anytime extended to include other modalities too, since our fusion strategy is independent of the input modality. To be specific, we employ a late decision-fusion strategy. This goes on aggregating frame-level and video-level predictions obtained from CNN and LSTM respectively of different modalities, until there remains a single prediction vector. This final probability vector acts as the prediction made by the CNN-LSTM architecture. To evaluate our fusion strategy, in Table 2, we have tabulated some of the recent techniques that employ multimodality fusion. While it is seen that most researchers (Wu et al., 2015; Li et al., 2020; Wang et al., 2016; Cherian & Gould, 2019, etc.) prefer to use the average fusion, few (Zhang & Xiang, 2020; Mazari & Sahbi, 2019) prefer other variants. It is certainly debatable and reliant upon a test of time, that which is the most effective and robust fusion strategy. But we have compared the efficacy of the various fusion methods, by how much it could increment the accuracy of individual streams. It is visible from Table 2 that, our fusion strategy could increment the highest individual modality score by 15.31%, 8.53%, 7.01% and 6.69% respectively on CCV, KCV, UCF-101 and HMDB-51 datasets. This %age improvement in accuracy surpasses all the tabulated SoTA methods in the first three datasets, but assumes a second position for HMDB-51 dataset.

Overall, we can conclude that an effective event and activity recognition method that drives a video surveillance system should possess an efficient temporal feature exploitation and an unparalleled multimodality fusion scheme. Both of these are necessary for a Cyber-Physical System (CPS) dedicated towards video surveillance.

5 Epilogue and Way Forward

A detailed insight into the problem of classifying activities and events for Cyber-Physical Systems (CPS) is provided in this work. From inception days to present-day advances, we talk at length about each the approaches that have grown over time, contemporarily forming the base of the solution framework on various grounds, their subsequent drawbacks and how the successive frameworks have made efforts to eradicate them as much as possible. We exhibit the prowess of solely using temporal motion features to characterize event classes, keeping aside the prejudiced notion of CNNs gracing the spatial information better. To effectively demonstrate the same, we resort to a hybrid model of a ResNet50-LSTM fusion. This considerably surpasses the state-of-the art methods exploit-

Table 2 Performance comparison of different approaches employing multimodality fusion, on each of the four datasets

Dataset	Method	Description	Fusion	Acc (%)
CCV (Jiang et al. 2011)	Wu et al. (2015)	ConvNet (spatial + temporal)	Average	75.80 (S + 00.80)
	Wu et al. (2015)	ConvNet + LSTM (spatial + temporal)	Average	81.70 (S + 03.80)
	Wu et al. (2015)	ConvNet + LSTM (spatial + temporal + acoustic)	Average	82.40 (S + 04.50)
	Li et al. (2020)	Spatio-temporal ResNet + hierarchical Attn	Average	74.21 (S + 08.14)
	Zhang and Xiang (2020)	GRU on transferred CNN	End-to-end network	75.10 (N/A)
	Ours (Jana et al. 2019)	**Key-Frame, Spatio-Temporal CNN+LSTM**	**Multi-tier conflation**	**81.89 (S + 15.31)**
KCV (Loui et al. 2007)	Wang et al. (2016)	HDCC + SIFT	Group-weighing	34.69 (N/A)
	Feng et al. (2014)	Multi-group adaptation n/w	–	44.70 (N/A)
	Ours (Jana et al. 2019)	**Key-frame, Spatio-Temporal CNN + LSTM**	**Multi-tier conflation**	**57.52 (T + 08.53)**
UCF-101 (Soomro et al. 2012)	Wu et al. (2015)	ConvNet (spatial + temporal)	Average	86.20 (S + 03.60)
	Wu et al. (2015)	ConvNet+LSTM (spatial + temporal)	Average	90.10 (S + 06.10)
	Wu et al. (2015)	ConvNet+LSTM (spatial + temporal + acoustic)	Average	90.30 (S + 06.30)
	Wang et al. (2016)	Spatio-Temporal ConvNets (temporal segment n/w)	Average	93.50 (T + 05.60)
	Mazari and Sahbi (2019)	3-D 2-stream (combined) + Temp. pyramid	Hierarchical aggregation	97.94 (T + 01.53)
	Peng et al. (2017)	Spatial ResNet152 + temporal ResNet50	Average	87.80 (S + 06.70)
	Zang et al. (2018)	Spatio-temporal ConvNet	Attention model	94.60 (T + 06.30)
	Zhang and Xiang (2020)	GRU on transferred CNN	End-to-end network	88.00 (N/A)
	Ours (Jana et al. 2019)	**Key-frame, Spatio-temporal CNN + LSTM**	**Multi-tier conflation**	**89.03 (S + 07.01)**
HMDB-51 (Kuehne et al. 2011)	Girdhar et al. (2017)	ActionVLAD (RGB + Flow) Streams	ActionVLAD Late-Fuse	66.90 (T + 07.80)
	Cherian and Gould (2019)	ResNet-152 (RGB + Opt-Flow + SMAID)	Average	63.50 (T + 04.00)
	Zhang and Xiang (2020)	GRU on transferred CNN	End-to-end network	59.10 (N/A)
	Li et al. (2020)	Spatio-temporal ResNet + Hierarchical Attn	Average	70.69 (S + 02.31)
	Ours (Jana et al. 2019)	**Key-frame, spatio-temporal CNN + LSTM**	**Multi-tier conflation**	**61.91 (S + 06.69)**

Evaluation is made based on average accuracy (Acc) over all classes, expressed in percentage. In the rightmost column, value in bracket indicates increment (+)/decrement (−) from the highest individual performance of a modality stream. S = spatial, T = temporal, A = acoustic

ing only action features, and is found to be comparable to some which make use of the visual cues offered by the frame images. Our multi-level fusion strategy uses the concept of biased conflation and takes into account verdicts from both the spatial and temporal wings of the network, as well as on the grounds of frame and video level predictions. It can be said that the robustness of this novel statistical method lies in the fact that it has the potential to effectively "fuse" two apparently wrong or disagreeing predictions obtained from the respective spatial and temporal wings to an eventual correct classification. This is observed as it undergoes various formative stages in the method of fusion. It may greatly help in practical scenarios of doubt in surveillance for a CPS. For example hypothetically, while the spatial content for a malicious intruder in an ATM booth would not vary that much as compared to a general customer, suspicious activities other than what is usually expected can be recognized by the temporal wing. The confidence of verdicts of both of these can then undergo the fusion process for the decision to be made by the model (so as to fire an alarm on detected intrusion or not). Apart from these merits, the model could be improved in dealing with classes having a high degree of semantic correlation (for example, Boxing and Punching, Soccer Juggling and Kicking). Modifications in the network model to account for such scenarios could be made. Also, we are yet to exploit auditory information in classifying these events. Finally, guiding the CNN or RNN model through an effective 'attention' scheme could add clarity to the way each activity class is characterized. This could be explored, along with constructing a suitable and generic interpretation for what could be exploited in this 'fovea' or 'attention' stream.

References

Alzubi, J., Nayyar, A., & Kumar, A. (2018). Machine learning from theory to algorithms: An overview. In: *Journal of Physics: Conference Series, 1142*.

Bhattacharyya, A. (1946). On a measure of divergence between two multinomial populations. *Sankhyā: The Indian Journal of Statistics*, 401–406.

Blank, M., Gorelick, L., Shechtman, E., Irani, M., Basri, R. (2005). Actions as space-time shapes. In *Proceedings of the Tenth IEEE International Conference on Computer Vision (ICCV'05)* (Vol. 2, pp. 1395–1402). IEEE.

Bobick, A. F., & Davis, J. W. (2001). The recognition of human movement using temporal templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *23*(3), 257–267.

Borisyuk, F., Gordo, A., & Sivakumar, V. (2018). Rosetta: Large scale system for text detection and recognition in images. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 71-79).

Cedras, C., & Shah, M. (1995). Motion-based recognition a survey. *Image and Vision Computing*, *13*(2), 129–155.

Chen, L., Duan, L., Xu, D.: Event Recognition in Videos by Learning from Heterogeneous Web Sources. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 2666–2673 (2013)

Cherian, A., & Gould, S. (2019). Second-order temporal pooling for action recognition. *International Journal of Computer Vision*, *127*(4), 340–362.

Dalal, N., & Triggs, B. (2005). Histograms of oriented gradients for human detection. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)* (Vol. 1, pp. 886-893). IEEE.

Derpanis, K. G. (2004). *The Harris corner detector* (pp. 1–2). York University.

Duan, L., Xu, D., & Chang, S. F. (2012). Exploiting web images for event recognition in consumer videos: A multiple source domain adaptation approach. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1338–1345). IEEE.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science*, *167*, 1950–1959.

Elgammal, A., Harwood, D., & Davis, L. (2000). Non-parametric model for background subtraction. In *Proceedings of the European Conference on Computer Vision* (pp. 751–767). Springer.

Feng, Y., Wu, X., Wang, H., & Liu, J. (2014). Multi-group adaptation for event recognition from videos. In *Proceeding of the 22nd International Conference on Pattern Recognition* (pp. 3915–3920). IEEE.

Ghosh, S., Kundu, A., & Jana, D. (2011). Implementation challenges of time synchronization in vehicular networks. In *Proceedings of the IEEE Recent Advances in Intelligent Computational Systems* (pp. 575–580). IEEE.

Girdhar, R., & Ramanan, D. (2017). Attentional pooling for action recognition. In *Proceedings of the Advances in Neural Information Processing Systems* (pp. 34–45).

Girdhar, R., Ramanan, D., Gupta, A., Sivic, J., & Russell, B. (2017). Actionvlad: Learning spatio-temporal aggregation for action classification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 971–980).

Gould, K., & Shah, M. (1989). The trajectory primal sketch: A multiscale scheme for representing motion characteristics. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (pp. 79–80). IEEE Computer Society.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access*, *8*, 24746–24772.

Hill, T. (2011). Conflations of probability distributions. *Transactions of the American Mathematical Society*, *363*(6), 3351–3372.

Horn, B. K., & Schunck, B. G. (1993). Determining optical flow: A retrospective. *Artificial Intelligence*, *59*, 81–87.

Jain, R., Nayyar, A., Bachhety, S. (2020). Factex: A practical approach to crime detection. In *Data management, analytics and innovation* (pp. 503–516). Springer.

Jana, D., & Bandyopadhyay, D. (2013). Efficient management of security and privacy issues in mobile cloud environment. In *Proceedings of the Annual IEEE India Conference (INDICON)* (pp. 1–6). IEEE.

Jana, D., & Bandyopadhyay, D. (2015). Controlled privacy in mobile cloud. In *Proceedings of the IEEE 2nd International Conference on Recent Trends in Information Systems (ReTIS)* (pp. 98–103). IEEE.

Jana, P., Bhaumik, S., & Mohanta, P. P. (2019). A multi-tier fusion strategy for event classification in unconstrained videos. In *Proceedings of the 8th International Conference on Pattern Recognition and Machine Intelligence (PReMI)* (pp. 515–524). Springer.

Jana, P., Bhaumik, S., & Mohanta, P. P. (2019). Key-frame based event recognition in unconstrained videos using temporal features. In *Proceedings of the IEEE Region 10 Symposium (TENSYMP)* (pp. 349–354). IEEE.

Jana, P., Ghosh, S., Sarkar, R., & Nasipuri, M. (2017). A fuzzy C-means based approach towards efficient document image binarization. In *Proceedings of the 9th International Conference on Advances in Pattern Recognition (ICAPR)* (pp. 332–337). IEEE.

Jiang, Y. G., Dai, Q., Xue, X., Liu, W., & Ngo, C. W. (2012). Trajectory-based modeling of human actions with motion reference points. In *Proceedings of the European Conference on Computer Vision* (pp. 425–438). Springer.

Jiang, Y. G., Ye, G., Chang, S. F., Ellis, D., & Loui, A. C. (2011). Consumer video understanding: A benchmark database and an evaluation of human and machine performance. In *Proceedings of the 1st ACM International Conference on Multimedia Retrieval* (pp. 1–8). http://www.ee.columbia.edu/ln/dvmm/CCV/. Accessed July 2020.

Kalra, G. S., Kathuria, R. S., & Kumar, A. (2019). YouTube video classification based on title and description text. In *Proceedings of the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 74–79). IEEE.

Karpathy, A., Toderici, G., Shetty, S., Leung, T., Sukthankar, R., & Fei-Fei, L. (2014). Large-scale video classification with convolutional neural networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1725–1732).

Kuehne, H., Jhuang, H., Garrote, E., Poggio, T., & Serre, T. (2011). HMDB: A large video database for human motion recognition. In *Proceedings of the International Conference on Computer Vision* (pp. 2556–2563). IEEE. https://serre-lab.clps.brown.edu/resource/hmdb-a-large-human-motion-database/. Accessed July 2020.

Laptev, I. (2005). On space-time interest points. *International Journal of Computer Vision*, *64*(2–3), 107–123.

Lee, J., Abu-El-Haija, S., Varadarajan, B., & Natsev, A. (2018). Collaborative deep metric learning for video understanding. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 481–490).

Li, Y., Liu, C., Ji, Y., Gong, S., & Xu, H. (2020). Spatio-temporal deep residual network with hierarchical attentions for video event recognition. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* **16**(2s), 1–21.

Liu, K., Li, Y., Xu, N., & Natarajan, P. (2018). Learn to combine modalities in multimodal deep learning. arXiv preprint arXiv:1805.11730.

Loui, A., Luo, J., Chang, S. F., Ellis, D., Jiang, W., Kennedy, L., Lee, K., & Yanagawa, A. (2007). Kodak's consumer video benchmark data set: Concept definition and annotation. In *Proceedings of the International Workshop on Multimedia Information Retrieval* (pp. 245–254). http://www.ee.columbia.edu/ln/dvmm/consumervideo/. Accessed July 2020.

Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, *60*(2), 91–110.

Lu, J., Hu, J., & Zhou, J. (2017). Deep metric learning for visual understanding: An overview of recent advances. *IEEE Signal Processing Magazine*, *34*(6), 76–84.

Luo, C., Jin, L., & Sun, Z. (2019). MORAN: A multi-object rectified attention network for scene text recognition. *Pattern Recognition*, *90*, 109–118.

Luo, M., Chang, X., Nie, L., Yang, Y., Hauptmann, A. G., & Zheng, Q. (2018). An adaptive semisupervised feature analysis for video semantic recognition. *IEEE Transactions on Cybernetics*, *48*(2), 648–660.

Mazari, A., & Sahbi, H. (2019). Human action recognition with deep temporal pyramids. arXiv preprint arXiv:1905.00745.

Mohanta, P. P., Saha, S. K., & Chanda, B. (2011). A model-based shot boundary detection technique using frame transition parameters. *IEEE Transactions on Multimedia*, *14*(1), 223–233.

Mukherjee, A., Jana, P., Chakraborty, S., & Saha, S. K. (2020). Two stage semantic segmentation by SEEDS and Fork Net. In *Proceedings of the IEEE Calcutta Conference (CALCON)* (pp. 283–287). IEEE.

Mukhopadhyay, M., Pal, S., Nayyar, A., Pramanik, P.K.D., Dasgupta, N., & Choudhury, P. (2020). Facial emotion detection to assess learner's state of mind in an online learning system. In *Proceedings of the 5th International Conference on Intelligent Information Technology* (pp. 107–115).

Oron, S., Bar-Hille, A., & Avidan, S. (2014). Extended Lucas-Kanade tracking. In *Proceedings of the European Conference on Computer Vision* (pp. 142–156). Springer.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of things technologies for elderly health-care applications. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 217–243). Elsevier.

Paul, S., Chaudhuri, S., & Jana, D. (2016). Increasing the fault tolerance of NameNode: A proposal for using DataNode as a secondary backup node. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6*(6), 416–422.

Peng, Y., Ye, H., Lin, Y., Bao, Y., Zhao, Z., Qiu, H., Lu, Y., Wang, L., & Zheng, Y. (2017). Large-scale video classification with elastic streaming sequential data processing system. In *Proceedings of the Workshop on Large-Scale Video Classification Challenge* (pp. 1–7).

Pinar, A. J., Rice, J., Hu, L., Anderson, D. T., & Havens, T. C. (2016). Efficient multiple kernel classification using feature and decision level fusion. *IEEE Transactions on Fuzzy Systems*, *25*(6), 1403–1416.

Polana, R., & Nelson, R. (1994). Detecting activities. *Journal of Visual Communication and Image Representation*, *5*(2), 172–180.

Potter, M. C. (1976). Short-term conceptual memory for pictures. *Journal of Experimental Psychology: Human Learning and Memory*, *2*(5).

Priyadarshni, V., Nayyar, A., Solanki, A., Anuragi, A. (2019). Human age classification system using K-NN classifier. In *Proceedings of the International Conference on Advanced Informatics for Computing Research* (pp. 294–311). Springer.

Rana, M. A. T. (2011). Kernel and classifier level fusion for image classification. University of Surrey. https://books.google.co.in/books?id=24udAQAACAAJ.

Rother, C., Kolmogorov, V., & Blake, A. (2004). GrabCut: Interactive foreground extraction using iterated graph cuts. *ACM Transactions on Graphics (TOG)*, *23*(3), 309–314.

Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., et al. (2015). Imagenet large scale visual recognition challenge. *International Journal of Computer Vision*, *115*(3), 211–252.

Saeed, F., Paul, A., Karthigaikumar, P., & Nayyar, A. (2019). Convolutional neural network based early fire detection. *Multimedia Tools and Applications*, 1–17.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IoT applications under shadow-fading conditions. *Procedia Computer Science*, *167*, 1515–1523.

Sharma, P., Singh, A., Raheja, S., & Singh, K. K. (2019). Automatic vehicle detection using spatial time frame and object based classification. *Journal of Intelligent & Fuzzy Systems*, *37*(6), 8147–8157.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K., Choudhary, P., & Vashist, P. C. (2020). Internet of things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth*, *2*, 191.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020). Internet of things in pharma industry: Possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Elsevier.

Soomro, K., Zamir, A. R., & Shah, M. (2012). UCF101: A dataset of 101 human actions classes from videos in the wild. arXiv preprint arXiv:1212.0402. https://www.crcv.ucf.edu/data/UCF101.php. Accessed July 2020.

Tanwar, S. (2020). Fog data analytics for IoT applications-Next generation process model with state-of-the-art technologies. *Studies in Big Data*, *76*, 1–497.

Ukil, A., Jana, D., & De Sarkar, A. (2013). A security framework in cloud computing infrastructure. *International Journal of Network Security & Its Applications*, *5*(5), 11–24.

Varior, R. R., Shuai, B., Lu, J., Xu, D., & Wang, G. (2016). A Siamese long short-term memory architecture for human re-identification. In *Proceedings of the European Conference on Computer Vision* (pp. 135–153). Springer.

Wang, H., Wu, X., & Jia, Y. (2016). Heterogeneous domain adaptation method for video annotation. *IET Computer Vision*, *11*(2), 181–187.

Wang, H., Ullah, M. M., Klaser, A., Laptev, I., & Schmid, C. (2009, September). Evaluation of local spatio-temporal features for action recognition. In *Proceedings of the British Machine Vision Conference (BMVC)* (pp. 124.1–124.11). BMVA Press.

Wang, L., Xiong, Y., Wang, Z., Qiao, Y., Lin, D., Tang, X., & Van Gool, L. (2016). Temporal segment networks: Towards good practices for deep action recognition. In *Proceedings of the European Conference on Computer Vision* (pp. 20–36). Springer.

Wu, Z., Jiang, Y. G., Wang, X., Ye, H., Xue, X., & Wang, J. (2015). Fusing multi-stream deep networks for video classification. arXiv preprint arXiv:1509.06086.

Zang, J., Wang, L., Liu, Z., Zhang, Q., Hua, G., & Zheng, N. (2018). Attention-based temporal weighted convolutional neural network for action recognition. In *Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations* (pp. 97–108). Springer.

Zhang, L., & Xiang, X. (2020). Video event classification based on two-stage neural network. *Multimedia Tools and Applications*, 1–16.

An IoT-Based Autonomous Robot System for Maize Precision Agriculture Operations in Sub-Saharan Africa

Jibril Abdullahi Bala, Olayemi Mikail Olaniyi,
Taliha Abiodun Folorunso, and Emmanuel Daniya

Abstract

The importance of agriculture to the economic growth in sub-Saharan Africa suffers from several challenges. One of the major problems faced by the sector is the lack of suitable technology to optimize yield and profit to reduce the reliance of farmers on manual techniques of farming which is accompanied by drudgery, wastage, and low yields. Precision agriculture has been applied to maximize agricultural outputs while minimizing inputs. This study presents the design of an Internet of things (IoT)-based autonomous robot system that can be used for precision agricultural operations in maize crop production. The robot consists of a camera for remotely monitoring of the environment and a tank incorporated with a liquid level sensor which can be used for irrigation and herbicide application. The real-time feed from the camera as well as the output from the liquid level sensor is accessed from a cloud database via a Web application. This system can be adopted for improved crop production which in turn will increase crop yield, profit, and revenue generated from agriculture.

Keywords

Artificial intelligence • Fuzzy logic • Image processing • Internet of things • Precision agriculture • Robot navigation

1 Introduction

1.1 Background of the Study

In the twenty-first century, there has been a rapid growth in the information and communication technology (ICT) sector. This development has influenced human operations and industrial services. One of the most important developments in the ICT sector is the introduction of the Internet (Yusuf et al., 2019). Internet of things (IoT) is a system of interconnecting computing devices that are interrelated. These devices can transfer data over a network with the absence of human involvement (Iwayemi, 2018). The IoT is a network of physical devices, objects, buildings, people, animals, and other items that are embedded with sensors, software, electronic devices, and network connectivity that supports communication, collection, and exchange of data (Dubey et al., 2020; Nayyar and Puri, 2016a, 2016b; Padikkapparambil, 2020; Singh et al., 2020a, 2020b; Tanwar 2020a, 2020b). This technology allows devices to be remotely controlled and sensed using network infrastructure. This process allows the integration between the physical world and computer systems, which in turn, results in improved economic benefits, efficiency, effectiveness, and accuracy (Amadin et al., 2017). The IoT has a wide range of applications in various sectors including agriculture.

The Food and Agriculture Organization (FAO) estimated a 70% increase in global food production by the year 2050 (Ishengoma & Athuman, 2018). Also, the population of the African continent is projected to reach 2 billion by 2050 (Ishengoma & Athuman, 2018). Feeding this population would be quite challenging with limited farming methods. Currently, farmers in sub-Saharan Africa cultivate less area of land and harvest less due to a lack of technological development in the agricultural sector. Besides, traditional farming techniques predominantly used in the region results in low crop yield compared to mechanized farming methods. Africa has 25% of the world's arable land, yet it contributes

J. A. Bala (✉) · T. A. Folorunso
Department of Mechatronics Engineering, Federal University of Technology, Minna, Nigeria
e-mail: jibril.bala@futminna.edu.ng

O. M. Olaniyi
Department of Computer Engineering, Federal University of Technology, Minna, Nigeria

E. Daniya
Department of Crop Production, Federal University of Technology, Minna, Nigeria

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_5

only 10% of the global agricultural output (Ishengoma & Athuman, 2018).

Nigeria is West Africa's largest economy, and second largest in sub-Saharan Africa. The country is vast with approximately 68 million hectares of arable land, 12.6 million hectares of freshwater supplies, and an ecological diversity that provides the supplies required to produce and grow a wide variety of crops (Ewetan et al., 2017). Agriculture makes approximately a quarter of Nigeria's overall nominal gross domestic product (GDP).

In Nigeria, maize has evolved from a backyard crop to the third most important crop in terms of output and the area cultivated. Nigeria is the leading producer of maize in West Africa and the tenth-largest producer in the world. The 2008 FAO statistics reported that about 7.5 million tons of maize with an average yield of 1.9 metric tons per hectare produced in the country (Ammani, 2015). The crop is recognized as a major source of food and cash income among Nigerian farmers. Although the production of maize significantly increased in Nigeria between 1990 and 2011, an increase in population which leads to an increase in demand results in the need for improved maize production in the region (Ammani, 2015).

Precision agriculture (PA) highlights the fact that an understanding of variability within a crop field will achieve increased agricultural production. The goal is not to obtain the same outputs or yields all over the farm, but to evaluate the environment and distribute different site-specific inputs. This method can optimize agricultural benefits and produce a strong return on investment (Banu, 2015). In PA, the gap between mechanized farming and ICT is bridged by collecting farmland information and applying data analysis-based inputs. Farm operations such as application of herbicides, fertilizers, and irrigation can be done smartly, enabling farmers to achieve high yields, exact inputs use, reduce wastage, and maximize income (Beluhova-Uzunova & Dunchev, 2019).

The implementation of PA and IoT technologies has the potential to revolutionize the agricultural sector in sub-Saharan Africa. This study presents the conceptual design of an IoT-based autonomous robot system for maize production under precision agricultural operations. This system uses IoT, control, and AI technology to incorporate a smart, intelligent robotic device for precision maize farming. This system is expected to improve agricultural yield and profit, as well as bring a high return on investment for the region.

The remainder of the chapter is organized into four sections. Section 2 presents a review of existing literature including identified research gaps. The research implementation strategy and methodology is presented in Sect. 3. The expected results of the research are presented in Sect. 4 while the conclusion is given in Sect. 5.

1.2 IoT Advancements in Sub-Saharan Africa

The IoT development in the sub-Saharan African region has improved over the years as many African countries have already taken advantage of the technology. This stride can be seen in health care which tracks the health of their patients remotely to utility companies that monitor the usage of their resources for analytics purposes. However, despite the advancement in some sectors, the lack of suitable infrastructure makes it difficult for the region to make significant growth in areas that other developed nations find relatively easy (Ndubuaku & Okereafor, 2015a). West Africa has recently experienced rapid economic development with 90% of the population having access to mobile phones. With this trend, IoT has the potential of contributing immensely to various sectors (Dupont et al., 2018).

Several factors can lead to massive IoT deployment in numerous sectors. These include cost reduction for the majority of the products and services associated with IoT systems (Ndubuaku & Okereafor, 2015a). Other factors include:

i. Cheaper cost of bandwidth and sensors.
ii. Cheaper processing costs.
iii. Introduction and use of Big Data analytics.
iv. Widespread use of smartphones.
v. Cheaper and more accessible wireless networks.
vi. Alternative energy and low power technologies.

Despite the lag of IoT development in the sub-Saharan African region, there have been implementations of this technology in several areas across the region. These applications include vehicle tracking, air quality monitoring, railway tracks, and disease diagnosis in countries such as Kenya, Rwanda, South Africa, Nigeria, and Congo (Ndubuaku & Okereafor, 2015b).

The implementation of IoT systems in sub-Saharan Africa has been negatively affected by several factors which include low power supply, high poverty rate, network capacity constraint, illiteracy, absence of local content, low internet penetration, security challenges, cost of hardware and services, low ranges for rural access, dependency on proprietary infrastructure, and difficulty in deployment (Ndubuaku & Okereafor, 2015a; Dupont et al., 2018).

1.3 Problems of IoT Technology in Nigeria

In Africa, currently, the rate of adoption of IoT technologies is slow when compared to other continents. Nigeria, being the most populous country on the continent, has a large mobile market and, thus, numerous prospects in IoT implementation. Considering the benefits of IoT deployment, its implementation can lead to improved national and regional economic development and improve the standard of living of the populace (Ndubuaku & Okereafor, 2015b).

On one hand, several developed countries have adopted the use of IoT while harnessing the benefits of the technology. Yet, these developing countries have not fully utilized and adopted IoT platforms. For instance, in Nigeria, the impact of IoT is not widely conspicuous. This lack of prevalence of the technology has several causal factors ranging from illiteracy, poverty, and low level of awareness to the absence of facilitating conditions, especially in rural areas, where the need is more pronounced (Amadin et al., 2017).

There are a few other factors that significantly hinder IoT development in Nigeria. Low electric power supply impedes the implementation of smart technologies across the country. This lack of power supply, while being vital for industrial, technological, and economic growth, is prevalent across the nation (Iwayemi, 2018). Alternative energy sources have been explored by individuals, but the high involved in the installation of solar panels, inverters, and other power systems discourage populace from exploring these options.

Besides, the difficulty in procuring IoT devices has resulted in low IoT adoption across the country. Although the cost of sensors and processors have dropped over time, these devices are challenging to obtain, especially in the Nigerian market. Developers and researchers tend to order for the required devices online from outside the country. However, the time it takes for delivery is usually large and this discourages individuals from venturing into the field (Iwayemi, 2018).

With at least 48 million active Internet users, Nigeria remains a large market for IoT development (Adejuwon, 2018). Agencies such as the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission (NCC) have been developing infrastructures to enhance ICT development across the country. This stride in technology can be fully utilized to provide improved production and revenue across all sectors, including the agricultural sector.

1.4 IoT for Agricultural Development

In conventional farming, operations such as application of herbicide, fertilizer, and irrigation generally rely on the expertise of the farmer. While this knowledge is of the utmost value in farming, precision is not assured (Li et al., 2017). Considering conditions such as temperature, humidity, and illumination that are difficult to quantify and regulate, it is important to incorporate a method that not only tests certain parameters but also includes a mechanism for controlling them. The application of IoT in farming has immense benefits in optimizing production. Some potential areas that can be transformed by IoT in sub-Saharan Africa include pest and disease management, crop water management, food production and security, weed control, and smart greenhouses (Ishengoma & Athuman, 2018).

2 Review of Existing IoT Schemes in Agricultural Research

In the area of IoT-based smart agricultural systems, there exist several related works. In Pavithra (2018), an intelligent monitoring device for the agricultural greenhouse was presented. The system utilizes IoT infrastructure made up of nodes of a wireless sensor network to provide a monitoring feature for a greenhouse. The system monitors water level, temperature, soil moisture, humidity, and light intensity. However, it does not possess a control feature for remotely managing farm operations.

Similarly, Naresh and Munaswamy (2019) presented a smart agriculture system using IoT technology. The system makes use of a wireless sensor network to monitor power supply, soil moisture, humidity, temperature, and water levels. The system is controlled by an ARM 7 processor and transmits the data to a Web server via a Wi-Fi module. This system also does not possess a feature for remotely controlling the farm operations.

Ji et al. (2015) presented an IoT and mobile cloud-based architecture for smart planting. Here, a system initiative for remote monitoring of agricultural parameters was designed. The system uses technologies such as 3G, GPRS, and RFID to implement a remote monitoring feature. The data from the sensors can also be visualized via devices such as tablets and mobile phones. Although the design presented an architecture for the platform, no specific information was given regarding the techniques and schemes used in the design.

A smart agriculture IoT with cloud, fog, and edge computing techniques was presented in Nandhini et al. (2019). The proposed system utilizes a machine learning edge-based IoT system for remote monitoring of agricultural parameters. The technique provides low latency and secure connectivity for IoT operations. However, the system provides no remote-control techniques.

Furthermore, in Olaniyi et al. (2019), a remote monitoring and control system for poultry feed dispensing was presented. The system uses Global System for Mobile Communications (GSM) and Short Messaging Service (SMS) technologies to monitor and control poultry feed dispensing in a deep litter poultry farm. The system has an average response time ranging from 1.6 to 3.6 s depending on the network operator used. The system, however, had limited coverage due to its use of SMS and has the potential of being improved upon with Wi-Fi technologies.

A review of the state-of-the-art IoT in protected agriculture was presented in Shi (2019). The study did a literature survey on existing technologies as well as the limitations of current schemes. Although several IoT-based systems exist for agricultural operations, there also exists significant challenges in the field. These challenges include but are not limited to network issues, hardware and software challenges in terms of cost, durability, availability, security challenges, and environmental factors.

Similarly, in Ayaz et al. (2019), a review on IoT-based smart agriculture is presented. The authors explored the use of unmanned aerial vehicles (UAVs), sensors, and communication techniques for the development of a smart agriculture system based on IoT. Based on the review carried out, the authors noted that the use of IoT to boost agriculture is not optional, but necessary.

Based on the aforementioned review, the following research gaps were identified:

i. The absence of a mechanism for remote control of farm operations.
ii. The use of technologies with a limited range of accessibility.
iii. The absence of automation in systems that do not provide remote-control features.
iv. The lack of artificial intelligence is incorporated into the decision-making process.

Based on these findings, this study presents a conceptual design of an autonomous robot system based on IoT for maize precision farming operations in sub-Sahara Africa. This system uses IoT, control, and AI technologies to implement a smart and intelligent robotic system for maize precision farming.

3 Proposed Solution and Research Implementation Strategy

3.1 System Description and Characterization Model

The proposed system architecture is presented in Fig. 1. The system is controlled by Raspberry Pi 3 microcontroller. This controller serves as the central processing unit of the system. The inputs to the microcontroller are the images acquired from the camera module, the level of the liquid tank, and the remote commands received via the Wi-Fi module. The outputs of the microcontroller are the position of the servomotor for navigation, the speed of the DC motor for movement, the pump action of the DC pump for spraying, and the transmitted data for the Web application sent via the Wi-Fi module. The microcontroller runs a Mamdani-based fuzzy logic control algorithm for navigation, and an image-processing algorithm for determining the edges of the ridges in the farm environment. The controller also works bi-directionally with the Wi-Fi module to transmit and receive data from the Web application via the IoT cloud platform.

Figure 2 shows the steps of operation of the robotic system. Table 1 shows the technical information of the hardware design considerations. These major components are used in the design of the system. The table highlights the hardware considerations as well as the component ratings.

3.2 Autonomous Robot Navigation and Control Scheme

Hough Transforms for Ridge Detection

For the robot to move effectively between the ridges, there needs to be a technique for identification of the ridges. In this study, the technique of Hough transforms is implemented to detect the ridges in the farm environment. This technique is selected because Hough transform is one of the most common and widely used techniques used for line detection (Arce et al., 2017; Aminuddin et al., 2017). Hough transforms evaluate a unique equation at each point on an image where a possible line can be identified. Hough transforms based on the relationship are shown in Eq. 1.

$$\rho = x\cos\theta + y\sin\theta \qquad (1)$$

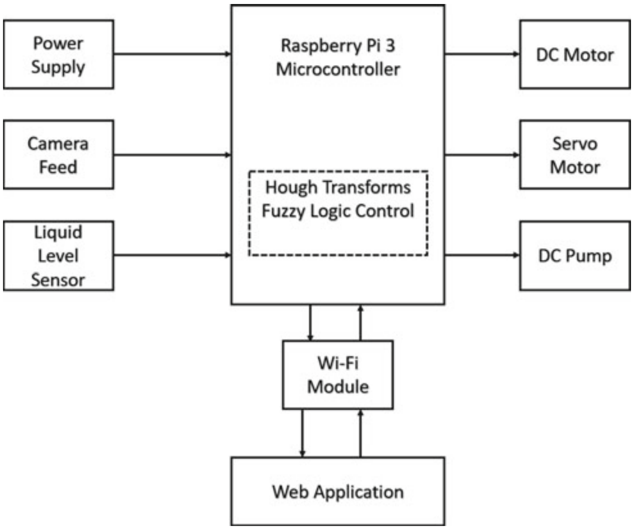


Fig. 1 Proposed system architecture

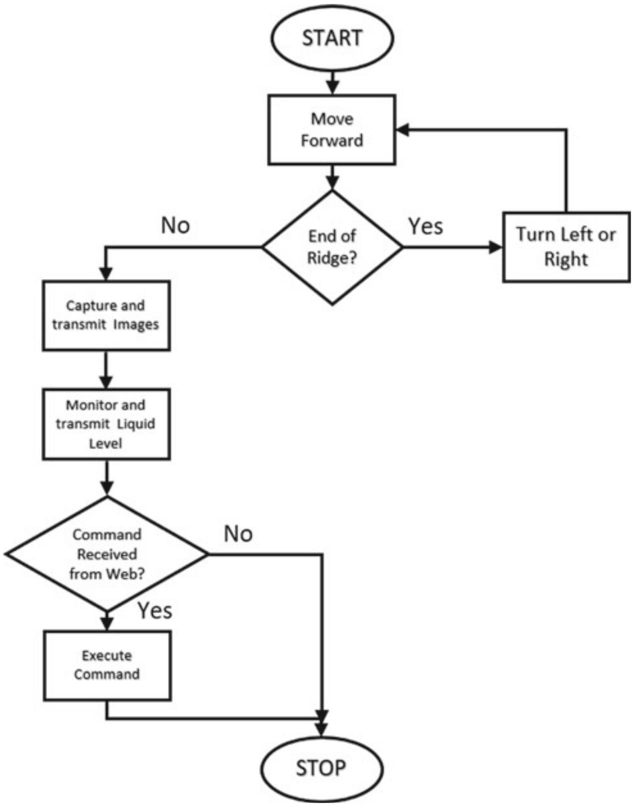


Fig. 2 Steps of operation of the robotic system

Table 1 Hardware technical information

Component	Rating
775 DC motor	12 V, 10,000 RPM, 80 W
FS5115M servomotor	5 V, 15.5 Kgcm
HQ camera	12.3 megapixels
Raspberry Pi 3 microcontroller board	Model B, 1 GB RAM, 1.2 GHz Quad Core
Wi-Fi module	802.11b/g/n
Liquid level sensor	CQRobot 5 V

The variables x and y indicate the coordinates of the image pixel. These coordinates are mapped to a corresponding parameter space in terms of ρ, which is the distance between the x-axis and the fitted line, and θ, which is the angle between the x-axis and the normal line (Li et al., 2018; Zheng et al., 2018). Figure 3 shows the mapping coordinate system of the Hough transform in terms of x, y, ρ, and θ.

The image-processing steps carried out in this system are highlighted in Fig. 4. First, the images of the farm area containing the ridges will be acquired from the camera module mounted on the front of the device. The camera will face downwards at a 45° angle. This will be done to capture the entire front view of the robot. Each video frame obtained will be processed as soon as the image is captured.

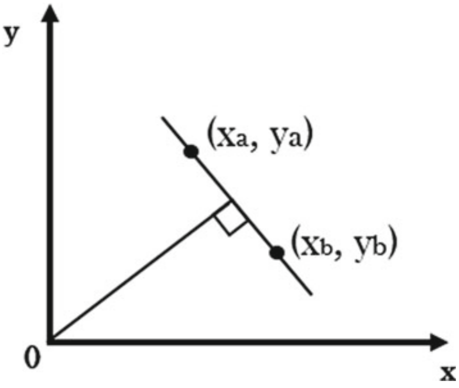


Fig. 3 Coordinate mapping of Hough transforms (Li et al., 2018)

After acquiring the image, the image is pre-processed before the desired features can be extracted. This image pre-processing involves identifying the regions of interest, noise removal, and image enhancement. The region of interest of the image is the lower half of the image. This area is selected to crop out the upper region which contains unwanted features such as the sky, grass, and crops.

Deleting noise from the image further processes the image. A median filter and a two-dimensional (2D) finite-impulse response (FIR) filter are used to accomplish this noise reduction. A median filter is used afterward in order to eliminate noise from the image while retaining the edges. This is useful for object detection since edge detection is a vital part of the algorithm. In addition, the 2D FIR filter removes noise from the image. However, it also sharpens and enhances the picture in addition to removing noise.

The next step after pre-processing an image is the segmentation of the image. In this study, the technique of segmentation implemented is the method of edge detection. This technique highlights the image's edges. In this case, the operator Sobel is used. The Hough transform algorithm is used when detecting the edges to get the lines detected in the image. Using Eq. 1, this algorithm identifies the ridgelines in the image. The machine then chooses the most prominent line as the ridgeline and the nearest line to the device.

When the nearest line is identified, the distance between the robot and the ridgeline is evaluated. This is done by calculating the distance between the middle of the camera and the line in terms of pixels. The value is then to the fuzzy logic controller for robot navigation.

Fuzzy Logic Controller for Navigation

The autonomous robot navigation scheme is carried out using a fuzzy logic controller (FLC) represented in Fig. 5.

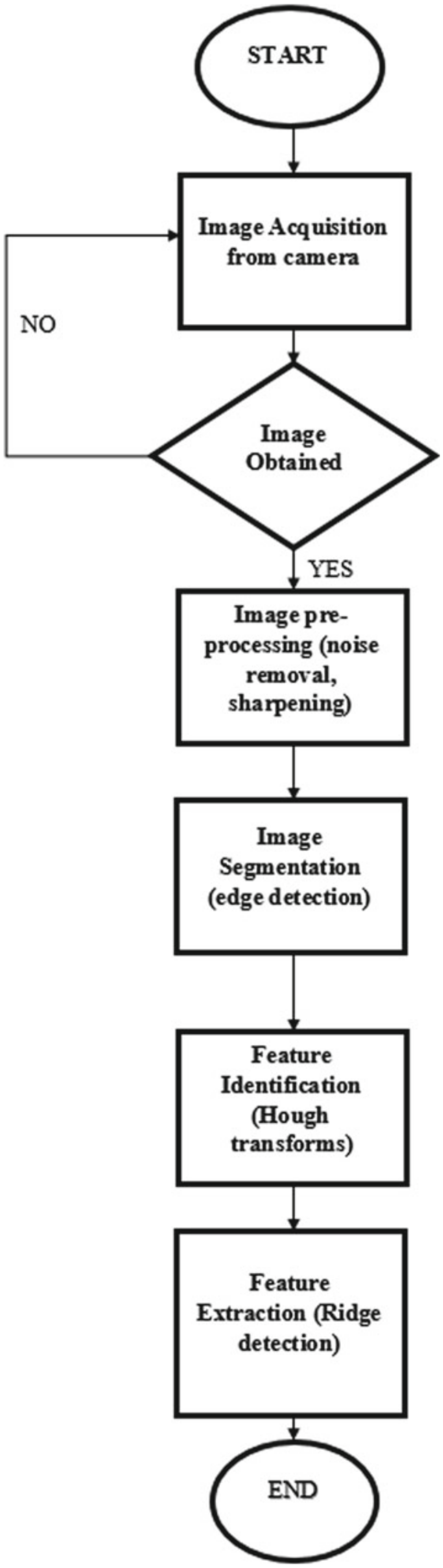


Fig. 4 Flowchart showing ridge detection process

The Mamdani fuzzy inference system (FIS) is adopted in this study due to its intuitiveness, wide acceptance, and suitability for a wide range of activities such as robot navigation. The inputs to the FIS are the position from the left ridge (leftPosition) and position from the right ridge (rightPosition) of the farm environment. The output of the FIS is the angle of the servomotor (servoAngle).

Fuzzification is the process of converting crisp inputs to fuzzy inputs and is achieved using membership functions (MFs). These functions map the crisp inputs to a value between 0 and 1. The triangular MFs are implemented for this design. There are three MFs used for each of the input and output variables. The MFs used for each of the inputs (rightPosition and leftPosition) are high, med, and low. In the case of the output, the MFs used are left, mid, and right. The input variables have ranges between 0 and 512. This value represents the pixel dimension of the camera. The output variable (servoAngle) has a range of −90 to 90, which represents the angle (in degrees) of the servomotor. The MFs of the inputs and outputs are shown in Figs. 6, 7, and 8.

After fuzzification is achieved. The inputs are converted to outputs via a set of fuzzy rules. These rules are in the form of Eq. 2.

$$\text{If } x \text{ is } A; \quad \text{then } y \text{ is } B \tag{2}$$

where A and B are linguistic variables. These types of variable are not numeric but are defined by fuzzy sets. The rules defined for this study are highlighted in Table 2.

After the rules are evaluated, the outputs are defuzzified to be converted from fuzzy outputs to crisp outputs. The defuzzification technique used for this design is the centroid technique. The crisp outputs will be passed to the microcontroller ports for actuator action.

3.3 IoT Platform Development

The IoT development platform is implemented with the Node-RED development tool developed by IBM. This choice is informed due to the platforms' ability to easily integrate with a Web application using APIs and JavaScript. The Node-RED runtime is built on node.js and the flows created are stored using JSON. Node-RED supports IoT development, and in this case, it is used together with the IBM cloud platform for the implementation of the remote monitoring and control features of the system.

The Node-RED implementation is done on the Raspberry Pi microcontroller. The controller is also connected to a 4G Wi-Fi shield for enhanced communication and Internet

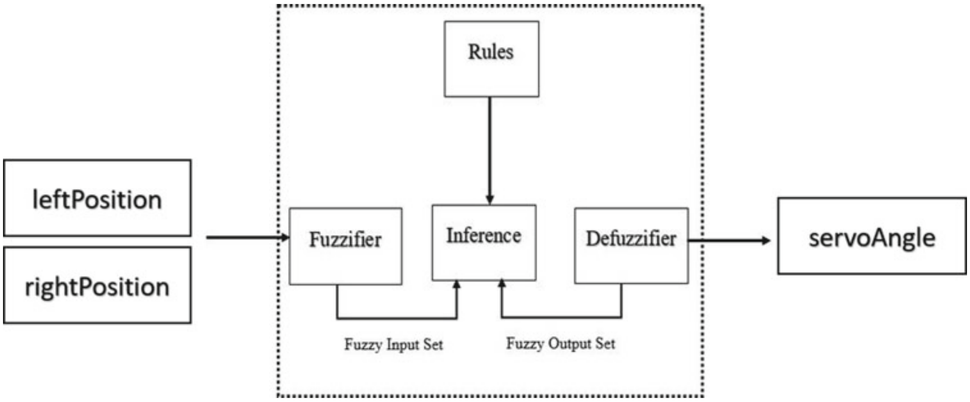


Fig. 5 Fuzzy logic controller

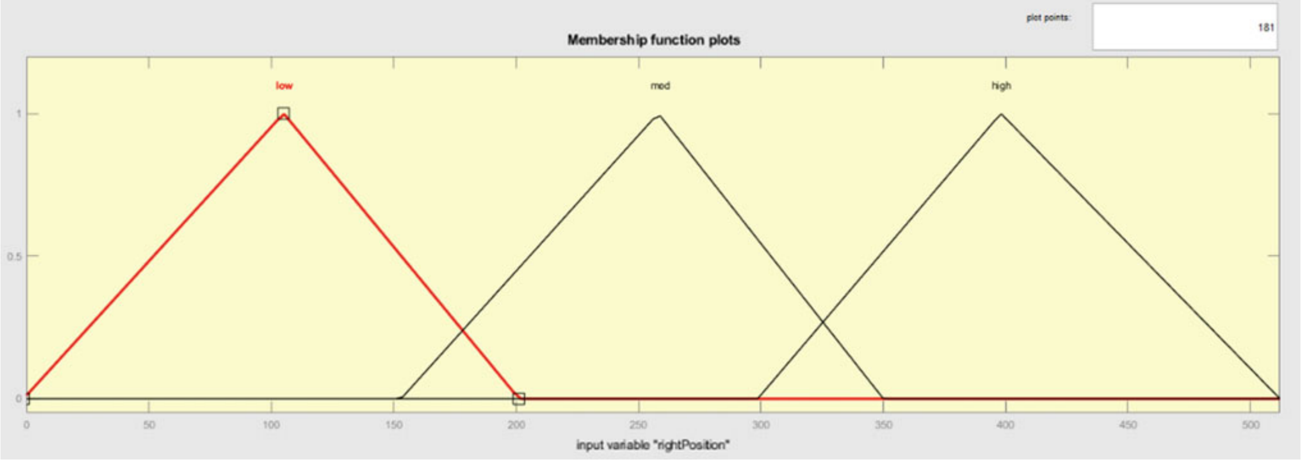


Fig. 6 Membership function for rightPosition

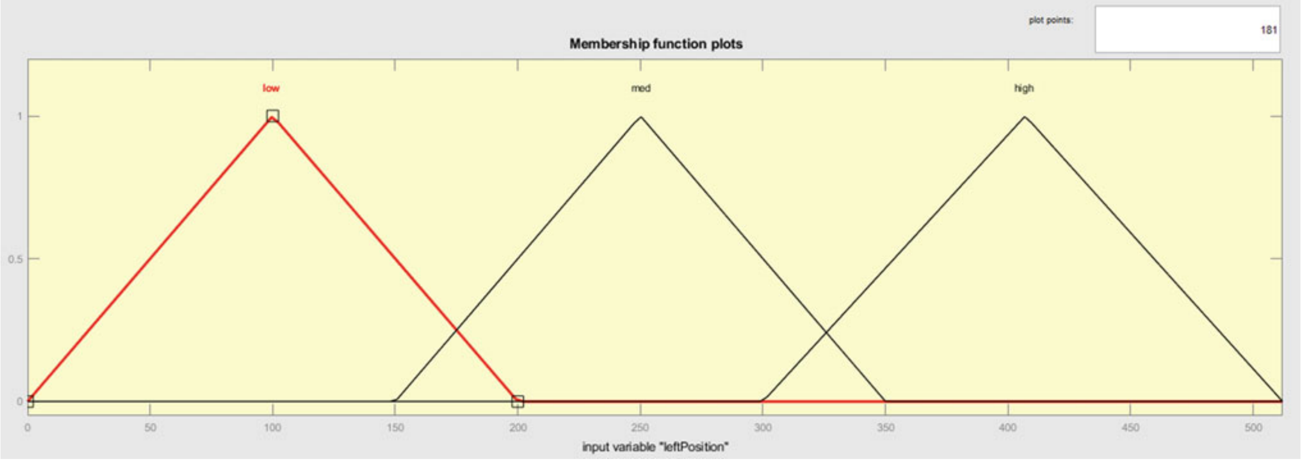


Fig. 7 Membership function for left position

connectivity. The architecture of the IoT platform is shown in Fig. 9. The microcontroller together with the Wi-Fi shield is the central hub of the platform. These interconnect with the sensors on the robot (liquid level sensor and camera module) to obtain data from the farm. The data is then transmitted through the Wi-Fi shield to the IBM cloud database. The Web application interfaces with the cloud to obtain the data and display it on the user interface.

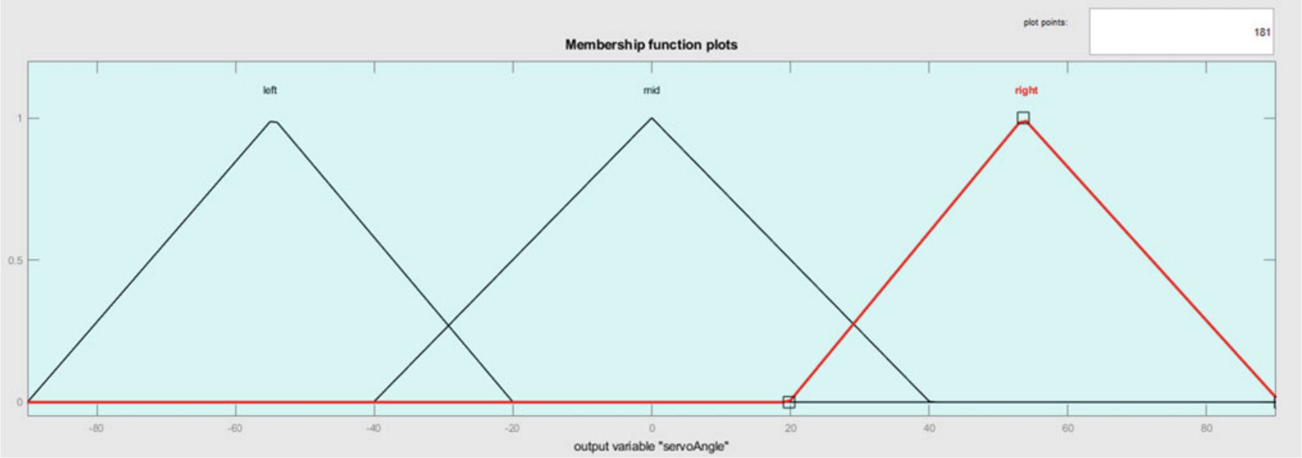
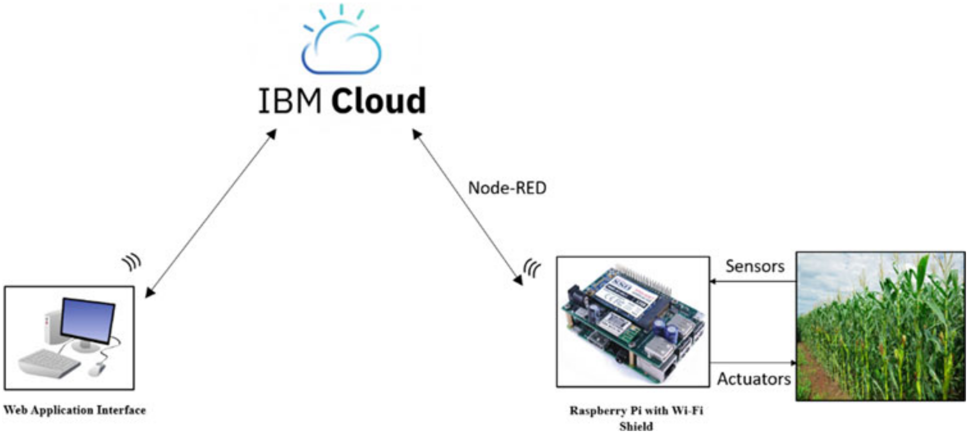


Fig. 8 Membership function for servoAngle

Table 2 Fuzzy rules

	LeftPosition			
RightPosition		Low	Med	High
	Low	Mid	Right	Right
	Med	Left	Mid	Right
	High	Left	Left	Mid

Fig. 9 IoT platform architecture



In addition to obtaining and displaying data from the farm, the IoT platform is also used to send command signals to the controller. Using bidirectional connectivity, the Web application is used to transmit signals to the controller through the cloud. These signals include DC pump action for spraying, servomotor position for navigation, and turning on or turning off the system. This feature enables a user to remotely control the robot's position and operations using the Web application interface.

3.4 Web Application Design

The Web application is developed to provide the user interface for remote monitoring and control. The application is developed using HTML, CSS, JavaScript, and PHP Web scripting languages. The Web application provides a graphical user interface for the visualization of farm parameters. These parameters include the liquid level of the robot tank and live feed from the camera. The application also provides an interface for remotely controlling the robot's actions. The operations that can be controlled are the robot's movement via the DC and servomotors, the robot's spray action via the DC pump, and the power status of the robot (On/Off).

4 Experimental Results

4.1 Prototype Development

The circuit diagram of the system is presented in Fig. 10. The robot is capable of moving automatically within the farm environment. The robot consists of three wheels, one in the front and two in the rear. The front wheel is powered by a servomotor which controls the direction of movement of the robot. The rear wheels are controlled by a DC motor, which is responsible for the forward motion of the robot. The camera module is mounted in the front of the robot for viewing the environment. The liquid tank incorporated with a liquid level sensor is placed at the back of the robot. The robot moves within a maize farm environment is shown in Fig. 11. The designed prototype is presented in Fig. 12.

Fig. 11 Maize farm environment

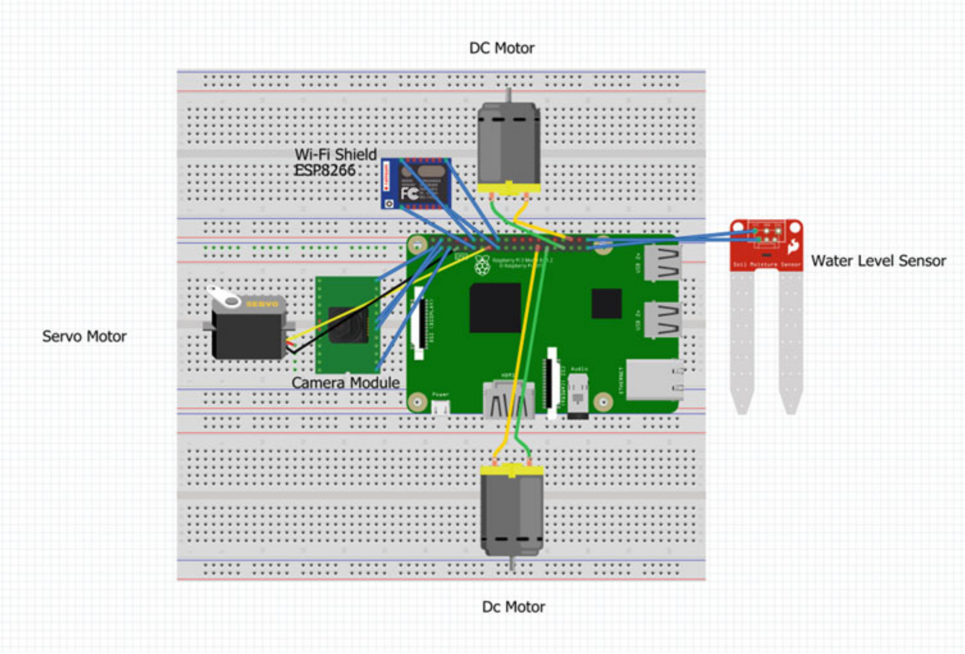
4.2 Ridge Detection, Robot Navigation, and Control

The results of the image-processing algorithm are shown in Fig. 13. In Fig. 13a, the original image acquired from the camera is shown. The image is pre-processed by converting to grayscale, enhancement, and noise removal. The results of the pre-processing are shown in Fig. 13b. Figure 13c shows the Sobel edge detection action on the image while the detected ridgelines using Hough transforms are shown in Fig. 13d.

After the ridgelines are detected and the distance from the robot is calculated, the value is sent to the fuzzy logic controller (FLC) for navigation. The expected trajectory of the algorithm is shown in Fig. 14. The fuzzy algorithm will steer the robot to the middle of the ridges and autonomously navigate within the farm ridges.

The surface view of the FLC is presented in Fig. 15. This shows the relationship between the inputs to the FLC and the output of the controller. The relationship and mapping

Fig. 10 Circuit diagram of the robotic system



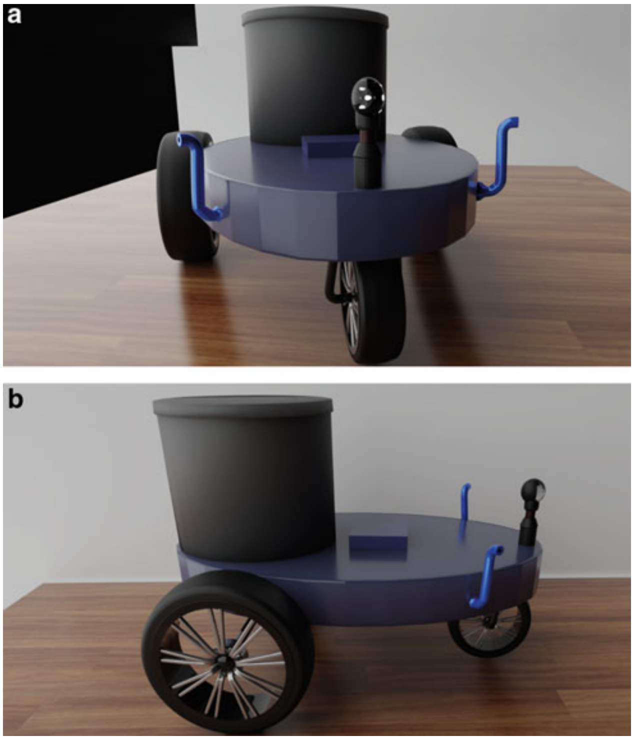


Fig. 12 **a** Designed robot prototype (front view), **b** designed robot prototype (side view)

between the inputs and outputs provide accurate and efficient movement within the environment.

4.3 Web Application

The layout for the Web application includes the features for remote monitoring and control as shown in Fig. 15. The application consists of a login page, as seen in Fig. 16a, to enable secure access and restrict unauthorized users. The dashboard, as shown in Fig. 16b, shows a summary of the robot including liquid level, spray action, and live camera feed. The user can also go to the control section to remotely control robot operations such as movement and spraying.

5 Conclusion

In sub-Saharan Africa, the potential of the agricultural sector can be enhanced through the adoption of precision agriculture to provide food and job security, increase income and revenues, and improve staple food crop production. Precision agricultural practices can be implemented to reduce human involvement in farming for the positive results in terms of increased crop yield and profit. The development of robotic farming systems is becoming widespread and the application of intelligent, autonomous, and smart solutions has been explored. Implementing the Internet of things (IoT) technology allows farmers the opportunity to be remotely present in their farms if they cannot physically be there. In this study, the conceptual design of an autonomous robot system based on IoT is presented for maize precision farming operations in a sub-Saharan Africa location.

The autonomous robotic system was designed using Node-Red, fuzzy logic, and Hough transform techniques. The robot consists of a camera mounted in front of it for capturing the front view of the robot. The image-processing algorithm based on Hough transforms processes the image to detect ridges in the farm. The distance of the robot from the ridges is fed into the fuzzy logic controller (FLC). The FLC processes the inputs, based on the fuzzy rules developed, and sends an output to the microcontroller for autonomous navigation. The live feed from the camera as well as the liquid level in the tank can be monitored remotely from a Web application using an IoT platform. This platform is developed using Node-RED and the IBM cloud. Also, the IoT platform provides a remote-control interface to control robot navigation and also control the spraying action of the pump. The system applies visual and sensory inputs to provide full functionality for farm operations.

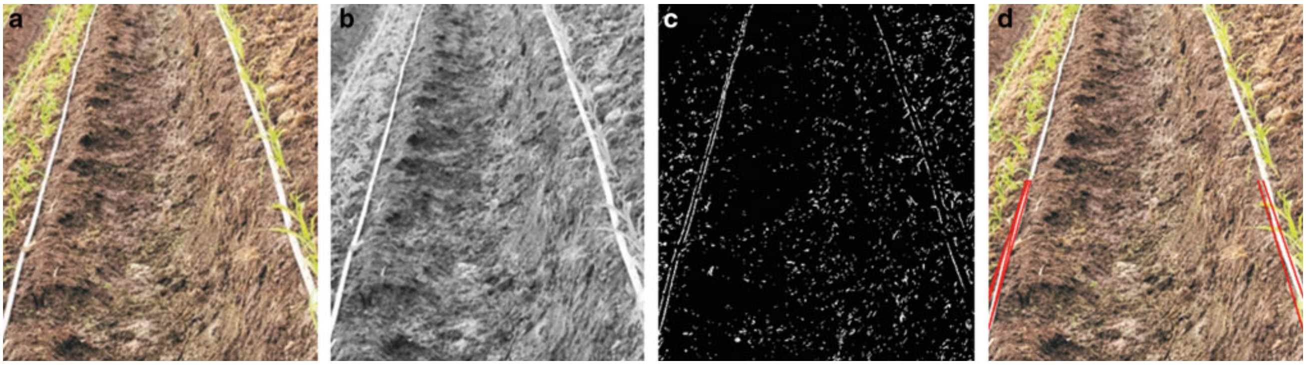


Fig. 13 **a** Original image, **b** pre-processed image, **c** edge detected image, and **d** ridge detected image

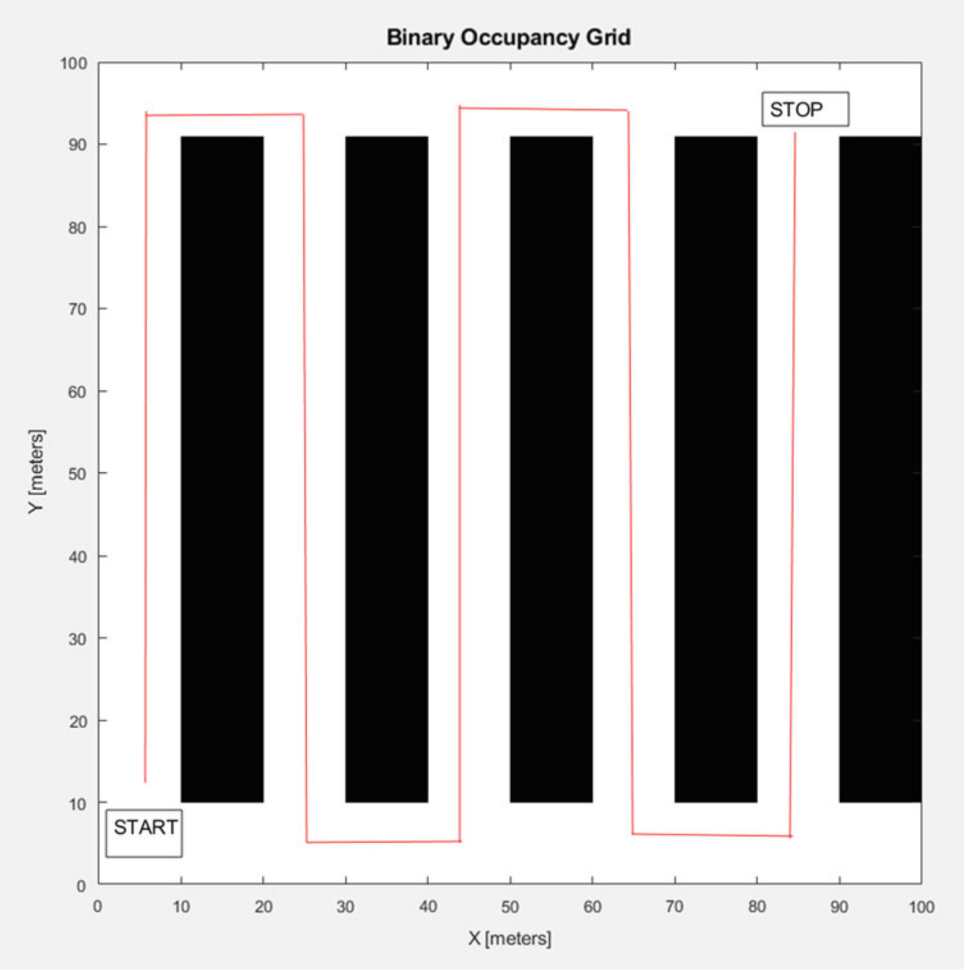


Fig. 14 Expected robot trajectory

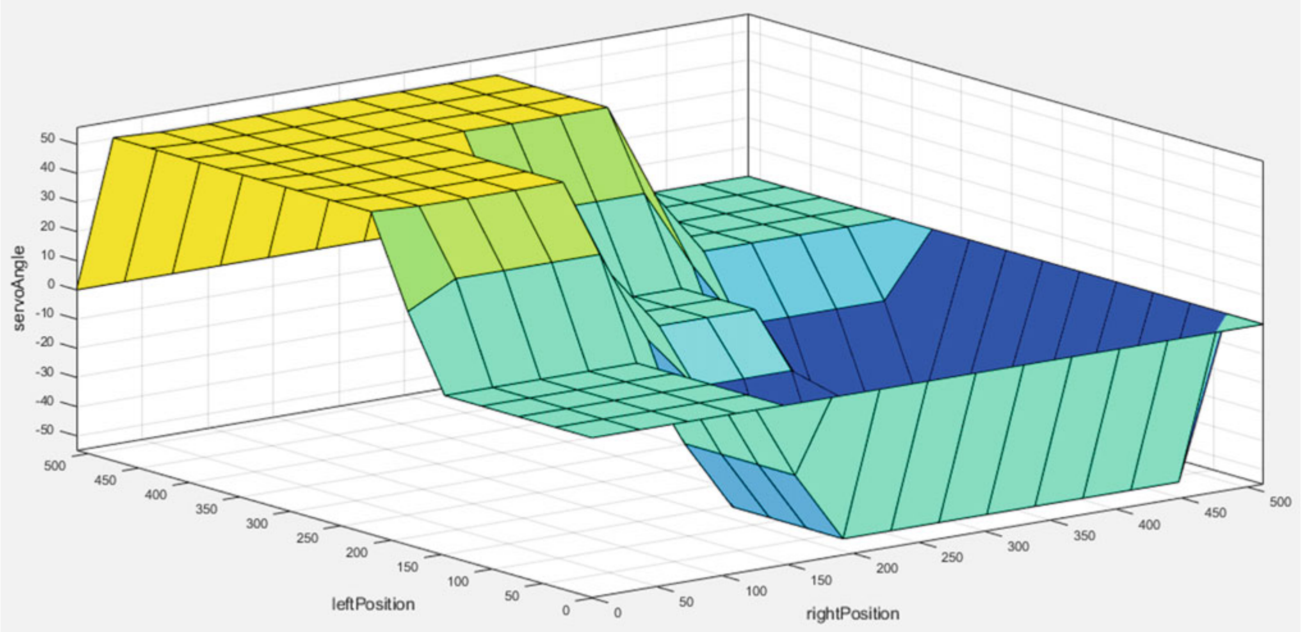


Fig. 15 Fuzzy surface view

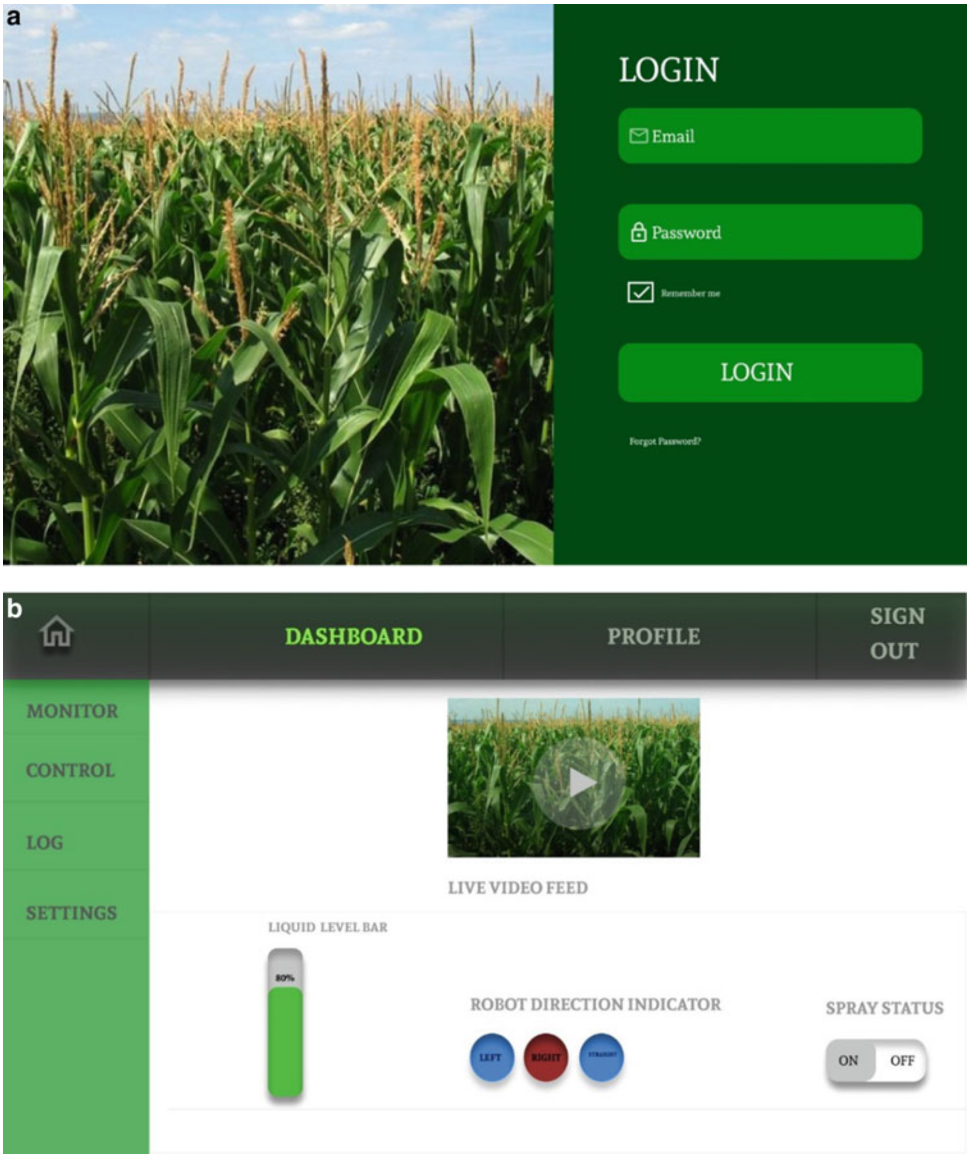


Fig. 16 **a** Web interface login page, **b** web interface dashboard

The system will allow farmers to cover large sections of arable land while minimizing human labor. Farmers will not find it necessary to hire a large workforce to cover their farmlands. This system will enable farmers to solely manage their farms. Furthermore, the system will enable remote monitoring and control of farm operations, especially in areas prone to disease outbreak, insecurity, and inaccessibility resulting from natural disasters and accidents.

Upon implementation and adoption, the system is expected to increase crop yield and profit while resulting in a decrease in human involvement and labor costs. In addition, the production of staple crop such as maize will be positively influenced as a result of the system's potential to encourage farming on a large scale. More revenue will be generated by the agricultural sector, thereby improving national and regional crop production.

Future areas that will be explored in this study are as follows:

i. Design Implementation and Prototype Fabrication: This involves the implementation of the designed algorithms on the microcontroller firmware, after which the performance of the implemented algorithms will be evaluated.
ii. Robot Assessment Accuracy Evaluation: This involves assessing the accuracy of the robot in terms of navigation, ridge detection, and communication with the Web application.
iii. Comparative Field Evaluation: Here, the performance of the robot will be compared with the conventional weed control and herbicide application techniques to determine the more effective scheme.

To stimulate agricultural growth, stakeholders and researchers in the agricultural sector must encourage the adoption of smart and intelligent farm technologies. However, the support in terms of research funding and the provision of secure communication channels to boost IoT applications will also go a long way in precision agriculture's technological growth. Farmers should be sensitized about the benefits of precision farming to encourage them to adopt new technologies for improved profit and yield.

References

Adejuwon, K. D. (2018). Internet of things and smart city development: Is Nigeria leveraging on emerging technologies to improve efficiency in public service delivery? *Journal of Public Administrative Finance Law, 13,* 7–20.

Amadin, F. I., Egwuatu, J. O., Obienu, A. C., & Osazuwa, W. A. (2017). Internet of things (IoT): Implications of a wide scale use in Nigeria. *Computer Information System Devices and Informatics Allied Research Journal, 8*(1), 95–102.

Aminuddin, N. S., Ibrahim, M. M., Ali, N. M., Radzi, S. A., Saad, W. H. M., & Darsono, A. M. (2017). A new approach to highway lane detection by using hough transform technique. *Journal of Information Communication Technology, 16*(2), 244–260.

Ammani, A. A. (2015). Trend analysis of maize production and productivity in Nigeria. *Journal of Basic and Applied Research International, 2*(3), 95–103.

Arce, F., Zamora, E., Hernández, G., & Sossa, H. (2017). Efficient lane detection based on artificial neural networks. *ISPRS Annals of the Photogrammetry Remote Sensing and Spatial Information Sciences, 4*(4W3), 13–19.

Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., & Aggoune, E.-H. M. (2019). Internet-of-things (IoT) based smart agriculture: Towards making the fields talk. *IEEE Access Specification Section New Technology Smart Farming 4.0 Research Challenges Opportunities, 7,* 129551–129583.

Banu, S. (2015). Precision agriculture: Tomorrow’s technology for today’s farmer. *Journal of Food Processing Technology, 06*(08), 8–13.

Beluhova-Uzunova, R., & Dunchev, D. (2019). Precision farming—Concepts and perspectives. *Problems of Agricultural Economics, 360*(3), 142–155.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Dupont, C., Vecchio, M., Pham, C., Diop, B., Dupont, C., & Koffi, S. (2018). An open IoT platform to promote eco-sustainable innovation in Western Africa: Real urban and rural testbeds. *Wireless Communication Mobile Computing, 2018,* 1–17.

Ewetan, O. O., Adebisi, F., & Emmanuel, O. (2017). Agricultural output and economic growth in Nigeria. *Journal of African Research Busines Technology, 2017*(2017), 1–11.

Ishengoma, F., & Athuman, M. (2018). Internet of things to improve agriculture in Sub Sahara Africa—A case study. *International Journal of Advertising Science and Research Engineering, 4*(6), 8–11.

Iwayemi, A. (2018). Internet of things: Implementation challenges in Nigeria. *American Journal of Engineering Research, 7*(12), 105–115.

Ji, C., Lu, H., Ji, C., & Yan, J. (2015). An IoT and mobile cloud based architecture for smart planting. In: *3rd international conference on machinery, materials and information technology applications (ICMMITA 2015)* (pp. 1001–1005).

Li, Z., Wang, J., Higgs, R., Zhou, L., & Yuan, W. (2017). Design of an intelligent management system for agricultural greenhouses based on the internet of things. In *Proceedings of 2017 IEEE international conference on computer science engineering IEEE/IFIP international conference embedded ubiquitous computing CSE EUC 2017*, vol. 2 (pp. 154–160).

Li, M., Li, Y., & Jiang, M. (2018). Lane detection based on connection of various feature extraction methods. *Advanced Multimedia, 2018,* 1–13.

Nandhini, S., Bhrathi, S., Goud, D. D., & Krishna, K. P. (2019). Smart agriculture IOT with cloud computing, fog computing and edge computing. *International Journal of Engineering Advanced Technology, 9*(2), 3578–3582.

Naresh, M., & Munaswamy, P. (2019). Smart agriculture system using IoT technology. *International Journal of Recent Technology Engineering, 7*(5), 98–102.

Nayyar, A., & Puri, V. (2016a, March). A review of Arduino board's, Lilypad’s & Arduino shields. In *2016 3rd international conference on computing for sustainable global development (INDIACom)* (pp. 1485–1492). IEEE.

Nayyar, A., & Puri, V. (2016b, September). Smart farming: IoT based smart sensors agriculture stick for live temperature and moisture monitoring using Arduino, cloud computing & solar technology. In *Proceedings of the international conference on communication and computing systems (ICCCS-2016)* (pp. 9781315364094-121).

Ndubuaku, M., & Okereafor, D. (2015) Internet of things for Africa : Challenges and opportunities. In *2015 international conference on cyberspace governance* (pp. 23–31).

Ndubuaku, M., & Okereafor, D. (2015). State of internet of things deployment in Africa and its future: The Nigerian scenario. *African Journal of Information Communication, 15,* 114–119.

Olaniyi, O. M., Buhari, U. U., Bala, J. A., Arulogun, O. T., & Kaa, T. O. (2019). Remote monitoring and control system for poultry feed dispensing. In *2019 IEEE 1st international conference on mechatronics, automation and cyber-physical computer system.*

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of things technologies for elderly health-care applications. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 217–243). Academic Press.

Pavithra, G. (2018). Intelligent monitoring device for agricultural greenhouse using IOT. *Journal of Agricultural Science and Food Research, 9*(2), 2–5.

Shi, X., et al. (2019). State-of-the-art internet of things in protected agriculture. *Sensors, 19,* 1–24.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth, 2,* 191.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020b). Internet of things in pharma industry: Possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Academic Press.

Tanwar, S. (2020a). *Fog computing for healthcare 4.0 environments: Technical, societal, and future implications, signals and communication technology* (1–622). Springer International Publishing.

Tanwar, S. (2020b). Fog data analytics for IoT applications—Next generation process model with state-of-the-art technologies. *Studies in Big Data, Springer International Publishing, 76,* 1–497.

Yusuf, F., Ifijeh, G., & Owolabi, S. (2019). Awareness of internet of things and its potential in enhancing academic library service delivery in a developing country. *Library Philosophy and Practice, 2831*.

Zheng, F., Luo, S., Song, K., Yan, C.-W., & Wang, M.-C. (2018). Improved lane line detection algorithm based on Hough transform. *Pattern Recognition Image Analysis, 28*(2), 254–260.

A Concept of Internet of Robotic Things for Smart Automation

R. Krishnamoorthy, Thulasi Bikku, V. Priyalakshmi, M. Amina Begum, and S. Arun

Abstract

A recent evolution in the field of Internet of Things (IoT) is the interdisciplinary domain involving smart automation and robotics implemented by the techniques of Internet of Things (IoT), famously known as Internet of Robotic Things (IoRT). This emerging technology is adopted in various sectors such as health care, manufacturing industries, economic, information technology and several other fields. Persistent sensors and actuators involved in robotics and automation are brought together by the emerging vision of Internet of Robotic Things. The domains of robotics and Internet of Things (IoT) cannot be viewed separately hence integrated together to form the novel domain—Internet of Robotic Things where the technologies of robotics are implemented in the scenarios of IoT. This chapter aims to provide an overview of possible solutions for various issues in smart automation environment and applications of robotics using Internet of Things (IoT). Envisioning dense heterogeneous devices communicating with each other to accomplish various objectives in the field of automation and robotics using Internet of Things (IoT) is the aim of this chapter. This technology can increase efficiency at reduced cost, significantly reducing manual intervention by increasing automation process visioning by SCADA systems. Industrial automation involving Internet of Things (IoT) has the goal of self-configuration, self-organization, self-healing system, scalability with less power consumption compatible to global standards. Involvement of robotics in the field of Internet of Things (IoT) potentially changes the process of production where the operations are performed rapidly in an accurate way leading to tremendous value in the field of automation. These two domains are converged and developed to provide the concept, architecture, involved technologies, challenges and applications and future work in order to cover (Internet of Robotic Things) IoRT comprehensively.

Keywords

Robotics • Industrial automation • Internet of robotic things • SCADA • Artificial intelligence • Smart environment • Industrial internet of things

1 Introduction

Development of next phase of applications of IoT will be provided by robotics, automation, swarm technologies and machine learning (Nayyar et al., 2017; Solanki & Nayyar, 2019; Batth et al., 2018). Conventionally, programmable dimensions are provided by the robotic systems in the machine design in order to perform work involving rich technologies for sensing and actuation while automation based on artificial intelligence for empowering the machine in making decisions and to learn algorithms (Anavangot et al., 2018; Singh et al., 2020a,b). Synergy of these technologies paves way for developing automation systems which integrates robotic in the IoT scenarios. Advanced level of artificial intelligence includes machine learning for

R. Krishnamoorthy · M. Amina Begum (✉)
Sree Sastha Institute of Engineering and Technology, Chennai, India
e-mail: amina.gtec@gmail.com

R. Krishnamoorthy
e-mail: krishnamoorthy.mkr@gmail.com

T. Bikku
Vignan's Nirula Institute of Technology and Science for Women, Guntur, India
e-mail: thulasi.jntua@gmail.com

V. Priyalakshmi
SRM Arts and Science College, Chennai, India
e-mail: kumaran.durairaj.kd@gmail.com

S. Arun
Prathyusha Engineering College, Chennai, India
e-mail: yesarun1810@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_6

performing autonomous system (Dubey et al., 2020; Sehgal et al., 2020; Padikkapparambil et al., 2020). Subsets of IoT discussed in this chapter are industrial IoT and robotic IoT where processes are improved by the interaction of the processing units, devices connected and the network with the involved environment for generating data (Singh et al., 2020c; Tanwar, 2020; Gupta et al., 2020). Realistic allocation of IoRT technology is done by IoT and functions of automation in this area. The increasing trend of robots which are centered on wireless communication to get connected with sensors, actuators and network resources has become common. Tremendous changes are brought by robotic system in the human society in various aspects of social and economic problems in the past decade (Siciliano and Khatib, 2008a).

Wide deployment is viewed by the robot manipulators in industries for performing critical and tedious job such as shield welding, assembling of product, packaging of boxes, car painting. Successful accomplishments are obtained by these preprogrammed robots in several applications in the industries due to precision, speed, accurate output and endurance. Technologies involved in robotics are integrated with the technologies of IoT in order to extend the applications of smart automation by deploying in both structured and unstructured environment for emerging the technology of robotics (Hu et al., 2012). In the current era, Internet of Things is an active research area, while robotics is a required and solid field of the industries for performing various tasks (https://www-users.cs.umn.edu/~isler/tc; Zhang et al., 2010). These two fields integrate together by the effort of the research communities. The technology of Robotics and IoT are integrated together for the realization of the technology Internet of Robotic Things (Kehoe et al., 2015; Kamei et al., 2012; Giusto et al., 2010; Smith, 2012). Related concepts to IoRT are organized such that reader is able to find it easier to identify from the coherent frame done in a coherent manner.

Aim of this chapter is to provide holistic vision between the technology of IoT and Robotics in the field of smart automation which forms the technology of Internet of Robotic Things (IoRT). A better understanding is provided on IoRT for identifying open issues that can be investigated by the research community. A comprehensive view is provided on the selected field for introducing the basic ideas to the reader behind robotics, smart automation and IoT.

The chapter is organized as follows. Section 2 focuses on providing an overview of Internet of Things which includes its definition in small environment and large environment. Section 3 describes the concept of Internet of Robotic Things along with its definition. Section 4 provides the architecture of Internet of Robotic Things representing various layers involved in it. Section 5 presents the concept of Artificial Intelligence and the various applications of it applied to make the environment to act smart. Section 6 describes the integration of smart environment with robotics to influence novel applications. Section 7 presents the computation requirements for implementing the applications with different types of computations. Section 8 describes the various cyber security issues in Internet of Robotic Things. Section 9 presents the application domains of Internet of Robotic Things. Section 10 provides the various applications of Internet of Robotic Things in industries. Section 11 describes the case studies of IoRT in industries. Section 12 presents the robotic applications aided by IoT. Section 13 concludes the chapter with future scope.

2 Concept of Internet of Things

This section provides a conceptual view of Internet of Things which includes origin of Internet of Things, novel definitions applicable for smaller environment and larger environment, categorization of IoT, fundamental characteristics of IoT along with its challenges.

The term Internet of Things is first coined by director of MIT, Kevin Ashton in the year 1999 while working on infrastructures of RFID (Radio Frequency Identification) where he used this term for reflecting his envision of electronic world where different devices are connected through a network and every electronic device is tagged with the data corresponding to it (IoT Definition, 2012). The Internet has its enhancement as Internet of Objects where the objects communicate data about themselves in order to get recognized. The objects are interconnected through the network, hence can collect information about other objects or can become blocks of other higher-level tasks. Let us proceed with the definitions of Internet of Things for smaller environment and larger environment.

2.1 Definition of IoT in a Scenario of Small Environment

"A connection of things which are identifiable uniquely connected to the internet through a network. The objects that are connected to the network have the capabilities of sensing, actuation and programmable in a potential manner. Unique identification is exploited for collecting the information about the object whose state can be varied at anytime, anywhere and anything" (Wan et al., 2016).

2.2 Definition of IoT in a Scenario of Large Environment

"Interconnection of large number of things through complex, adaptive network which can perform self-configuration is envisioned by usage of standard protocols through the network is termed as Internet of Things. These uniquely identifiable things are virtual representations which have the features of programmability, sensing and actuation. Accessible information is available about the things for the other objects such as location, identity, private or social information and status. Services are offered by the objects either with or without the intervention of human by exploiting the information captured, identity, sensing/actuation and communication capability through interfaces from anything, anytime and anywhere with proper security" (Wan et al., 2016).

Three categories of interaction are involved in IoT are,

(i) IoT for connecting person to person.
(ii) IoT for connecting person to machine/object.
(iii) IoT for connecting machine to machine/object.

Object indicates things which are locatable, readable, addressable and recognizable through the data of the sensors, controlled through Internet and compatible to various communication standards. Paradigms involved in IoT are Internet oriented indicating middleware, things oriented indicating the sensors and semantic oriented indicating knowledge. IoT is utilized in application domains belongings to these paradigms. The novel development of Internet is in the form of IoT where connection is established with objects anytime with any other thing at any place by anyone in the same network or business as shown in Fig. 1. Connectedness of IoT via gateway and network cloud is represented by schematic representation as shown in Fig. 2.

The special characteristics of IoT make it to rapidly penetrate in all the fields of our life which are discussed as follows:

(i) *Interconnectivity*: Objects in a network are compatible to get connected with each other through IoT hence the resources connected to the network are accessible to all the nodes connected to the network.
(ii) *Heterogeneous Communication*: Objects from different networks are able to communicate with other objects of different network and of different platforms making heterogeneity possible with the IoT devices.
(iii) *Large Range of Devices*: A large scale of devices can be connected to the IoT network for sharing data or interaction, such that numbers of devices or things connected are greater than that of current Internet service.
(iv) *Dynamic Range and Status*: IoT allows variability in the number of devices or things connected to it whose status can be changed dynamically such as change in speed or change in position etc.
(v) *Security*: Transfer of data from one node to other must be secured along with the personal data of the device creating a security paradigm which is scalable.
(vi) *Scalability*: Versatility and applicability should also be for smaller devices connected to IoT with accuracy similar to large scale devices.

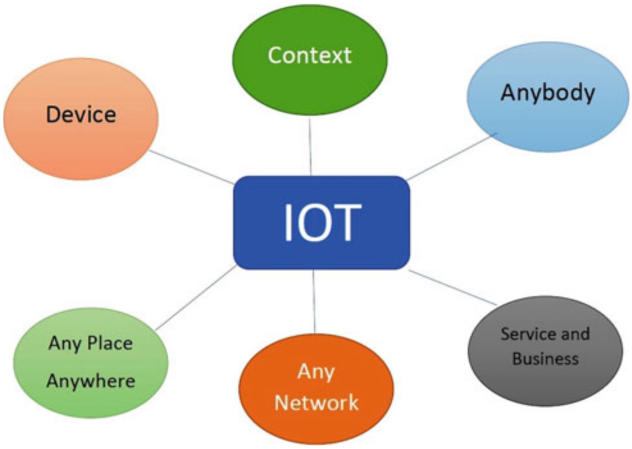


Fig. 1 Components of IoT

In fact, the above technologies such as heterogeneity or unique identification are not net but IoT leverages them for meeting the today's demand of the society such as technological or economic requirement. IoT performs the overall integration between human and machine which enables pursuing of decisions in real time by collaboration and communication technically. Great challenge of IoT is to secure data (Karjaluoto, 2006) either it belongs to the customer or belongs to the company but a different type of security is required by the customer data and the company data. Security requires IoT to monitor the devices connected and data in the network in real-time basis.

3 Concept of Internet of Robotic Things

This section provides a conceptual overview of Internet of Robotic Things (IoRT) which is obtained by merging Cloud Robotics with Internet of Things (IoT) presented in the previous section. IoRT is a novel concept combining IoT with robotics in specific Cloud Robotics hence we can represent IoRT as advanced level of Cloud Robotics.

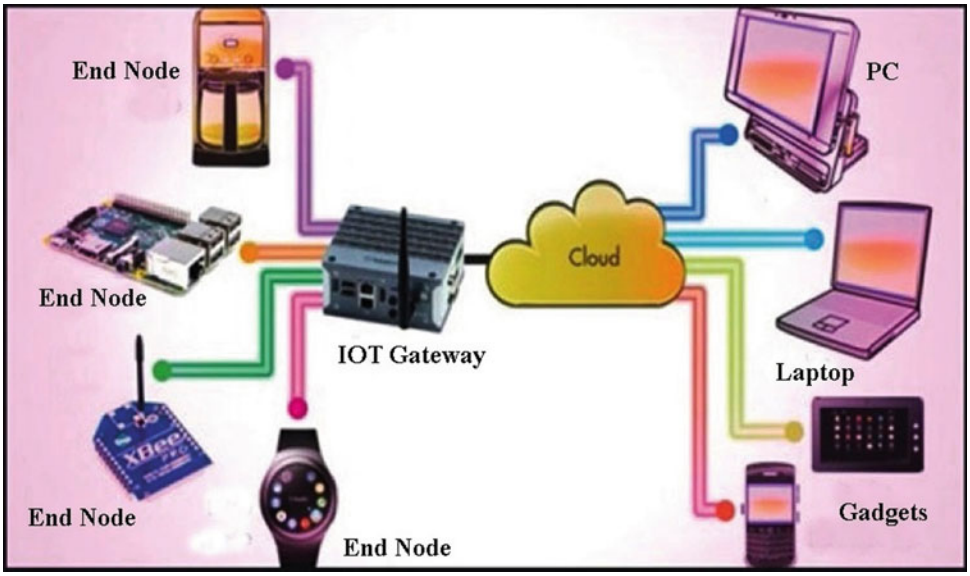


Fig. 2 Schematic representation of IoT

Cloud Robotics

Cloud Robotics is an emerging technology in the field of robotics which has taken its base from cloud computing, technologies of Internet, cloud storage system which aim to earn advantage of the infrastructure of the cloud system with its shared resources allowing the robotic systems to make use of efficient computation, cloud storage and latest communication platforms of the modern world connected with the cloud such that it can prevent robotic systems from over burdening such as updates, service maintenance, customizing platforms involves increased power consumption which is the main constrain for the mobility of the robot system thereby increases the cost of operation.

Let us proceed with the definition of Internet of Robotic Things (IoRT) which covers the definition of IoT and the definition of Cloud Robotics.

3.1 Definition of Internet of Robotic Things

A framework for the society of information and technology providing advanced services of robotics by integrating with Internet of Things based on the communication platforms, centered around cloud computing and cloud storage to extract benefits of shared resources of the cloud to allow robots to perform complex computation thereby removing maintenance overheads enhancing platforms of middleware to get customized with involving increased requirement of power, reducing the duration of operation thereby constraining the mobility of the robot making the task as hard real time with the concerned requirements (Henderson et al., 2016).

Hence, technologies of cognitive IoT integrates intelligence into processes in order to allow efficiency in business, creating new business opportunities thereby preparing IoRT systems in order to address variable requirements of environment which is more complex than IoT as shown in Fig. 3. The paradigm of Cloud Robotics is headed by Internet of Robotic Things which leverages few aspects such as virtualization from the technology of cloud computation and flexibility in novel designs of robotics via IoT with distributed computation, while differing from these technologies in some other aspects offering exceptional benefits and challenges in meeting the requirements.

4 Architecture of Internet of Robotic Things

In this section, different layers in the architecture of Internet of Robotic Things are described namely the hardware layer, the network layer, the Internet layer, the infrastructure layer and the application layer. Each of these layers is explained in the following sections as shown in Fig. 4.

4.1 The Hardware Layer

The layer which consists of various hardware such as sensors, robots, home appliances, industrial equipments, personal equipments, objects, smart phones, equipments used in defense, equipments operated underwater, weather sensors. Hence all the components of real life are included in this bottom most layer for providing data to the upper layer, the network layer.

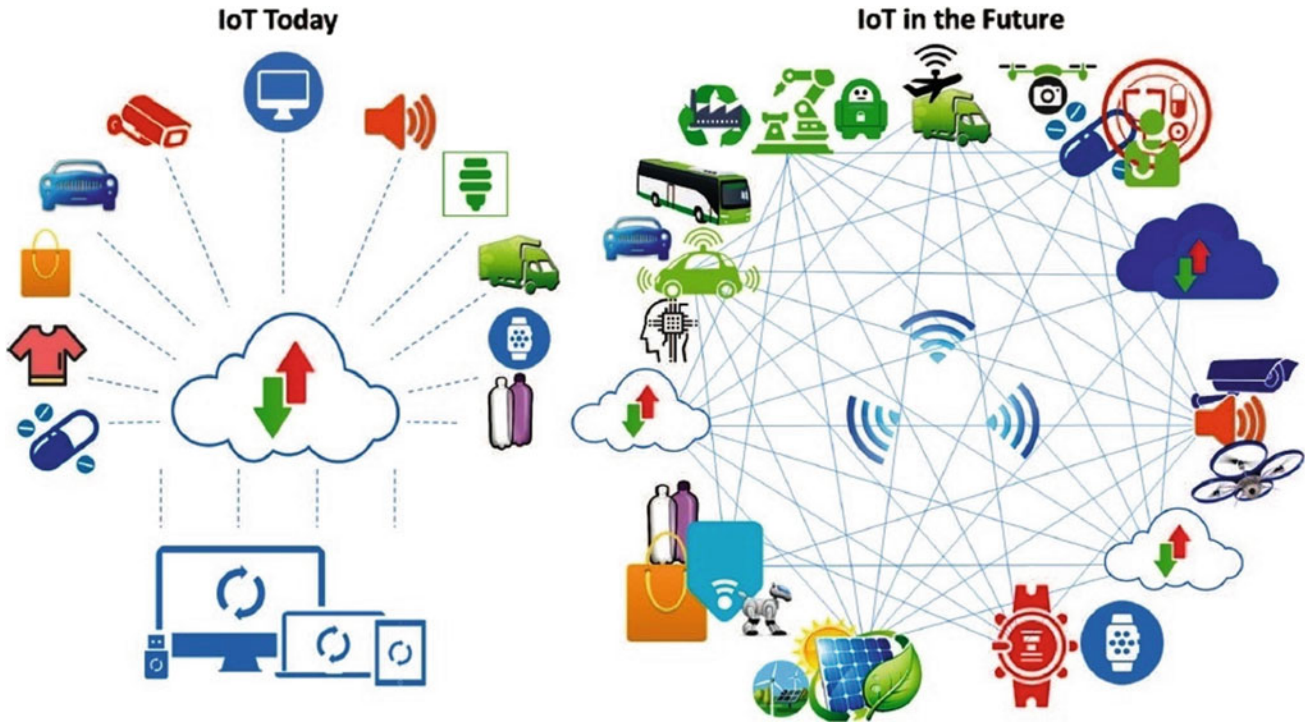


Fig. 3 Interconnection of devices in IoT and IoRT

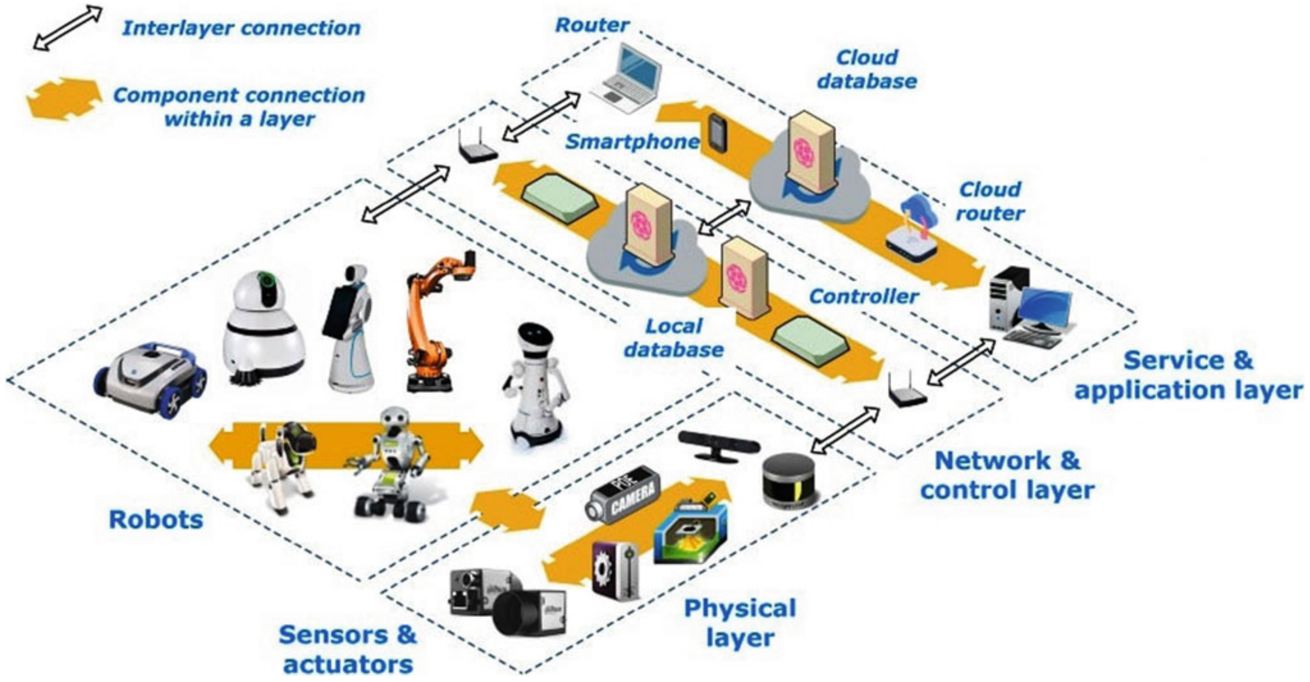


Fig. 4 Architecture of internet of robotic things

4.2 The Network Layer

The option for connectivity of various types of networks is possible by the network layer which is the second layer from the bottom. Connectivity in cellular networks such as 4G/LTE and third-generation cellular network are enabled by this layer. Communication technologies applicable for short range such as Bluetooth, Wi-Fi network, Broadband

Global Area Network, LoWPAN, Near Field Communication (Peng, 2012; Carpio et al., 2016; Ma & Luo, 2008; Fines et al., 2013; Chattha, 2014) are used to facilitate communication between the robotic things within a short range. Technologies used for communication for medium range includes Z Wave (Yarali & Ffahman, 2008; Yassein et al., 2016), Low Power Wide Area Network (Chi et al., 2016; Xue et al., 2016), Microwave Access, Zigbee for transmitting the data in the network of robots separated by long distance.

4.3 The Internet Layer

The central part of the architecture of IoRT is the connectivity via Internet. Communication protocols specific for IoT are included selectively in this layer for processing of information, efficiency of energy in the system of robotics. Various protocols involved in this layer are DDS, uIP, XMPP, UDP, MQTT, LLAP, DTLS, CoAP, AMQP, IPv6 (Campo et al., 2016; Schütz & Aschenbruck, 2016; Stanik & Kao, 2016; Pierleoni et al., 2016; Masirap et al., 2016; Fernandes et al., 2013; LLAP, 2020; Zhao & Liu, 2016; Ando et al., 2005) which performs task such as supporting multicast feature, networked embedded system dissemination, queuing of message in the middleware environment, automation in local network with lightweight, publishing messages, messaging instantly in real time, network with packet switching, alternate for TCP, datagram protocol with privacy and addressing real-time embedded systems directly for communication.

4.4 The Infrastructure Layer

This layer is a combined composition of five modules namely infrastructure of IoT Cloud Robotics, cloud platform for robotics, support for M2M2A cloud platform, services related to IoT business cloud and big data services. Each of the modules is discussed below:

Technologies specific for robot service such as ROS, RT, RSNP, CANOpen, ORiN and UNRPF (Saito et al., 2016; Arai & Matsuhira, 2016; Lastname et al., 2002; Postolache, 2016; Furrer et al., 2012) are provided by Robotic platform support. M2M2A indicates Machine to Machine to Actuator which provides paradigm for advance robot involved in IoRT system. A number of machines connected together through a network exchanging information with optimum automation control without the intervention of human are referred as Machine to Machine system. Leveraging of practical solution is through M2M2A where real world and virtual world are combined together by the technologies of sensors connected in the system and robotics.

In these solutions, information services that can be visualized obtained from the sensors have inter-linkage which formulates chain of reactions to be actuated by robots. Most important task includes collection of data, management of device, coordination of data from map and weather, analysis of data and accumulation of data by the sensors. Cloud Services related to IoT Business involves services specific to business manifestation for robots of IoT systems. Several transactions in business are served by the models of cloud service. Operations related to e-commerce are eased by the APIs which are oriented on modular business and packed business. IoRT are served by business clouds allowing manufacturers to diminish overheads on the business activities.

Infrastructures of IoT Cloud Robotics are involved based on the idea of IoT which facilitates advanced services by interconnection with things through technologies of communication accessing the network on demand with shared resources for computation (Kagaya, 2012). These resources can be provided with minimum effort as interaction between the service provider and the user is done in a well-defined manner. Hence, robotic systems are enabled by IoT cloud which involves services such as identification of location, SNS coordination, Scenarios with robotic behavior, image processing, Control over UI and video processing.

4.5 The Application Layer

This layer is designed for disseminating the experience of the user by exploration of present applications of robotics. Active participation can be taken by the robots bounded with IoT to solve problems that are related to fields such as data centers, maintenance of infrastructure, business shows, health care, EC sites, critical situations of life, WSDL interface (Ford, 2016) and supermarkets. There are endless possibilities which are of great importance in real-life time systems.

5 Artificial Intelligence

The field of artificial intelligence (AI) is related with intelligent machines rather than computers hence the field of science related to making of intelligent machines is known as artificial intelligence. In the industries of computers, AI is the significant element which helps in solving problems prevailing in the society. Computer programs, the expert systems are included in AI which simulates the performance and the reasoning of the human experts (Ray, 2016; Gao & Wu, 2014). Hence, embedded system is a computer application to solve the problems requiring the human expertise extensively. Simulation of human reasoning using particular rules represents the human expertise. Problems which fall in the AI framework are as follows:

- Proving of theorems.
- Problem solving.
- Machine learning.
- Playing of games.
- Natural language understanding.
- Recognition of patterns.
- Cognition and perception.
- Diagnosis of faults.
- Mathematics in symbolic method.
- Diagnosis in medical field.
- Expert control based on AI.
- Technological system restoration.
- Human reasoning simulation.

Artificial intelligence is built on the basics of philosophy, mathematics, biology and cognitive psychology. Various types of methods involved are methods based on knowledge, methods based on behavior and method of sub-symbolic which has technological content and scientific content. AI consists of non-exhaustive constituents as shown in Fig. 5.

The parts of robotics belonging to AI are the intelligent algorithms which perform the task of planning, navigation in local path/global path and controlling based on intelligence and knowledge. The process of AI that is conventionally used in Internet of Things is machine learning but it is tedious to define the process of machine learning as it involves new knowledge for the strategy of complex process or to rearrange the structure of the system in a proper way. Automated learning is the useful class under machine learning which is the capability of an intelligent system in enhancing the performance through intelligent learning based on the previous experience. In other way, learning of machines to operate and increase the efficiency by observation, classification and detection and correction of errors similar to human intervention is called as machine learning or artificial intelligence. Learning paradigms for automation involves five modules that are:

i. Learning of concept.
ii. Learning through examples or inductive learning.
iii. Learning through discovery.
iv. Learning through neural network.
v. Analogical learning.

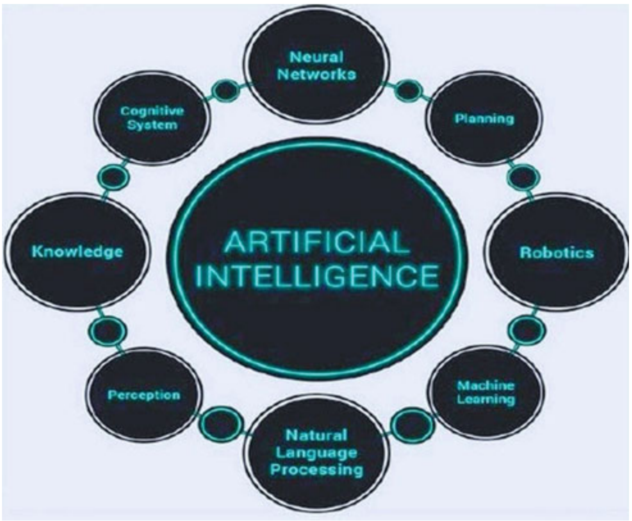


Fig. 5 Artificial intelligence and its constituents

Three systems of machine learning are as listed below:

a. Software system—IBM Watson which is a question answering system which provides answers based on machine learning.
b. Machine learning is used by Google cars for creating models of public on road.
c. Featured Recommendations of Amazon uses machine learning along with the past browsing history.

In the current era, smart machines are able to progress due the ability of artificial intelligence in handling previous task repetitively along with new task adapting itself to the changes of the task. Three stages are involved in the applications of AI which are as follows:

Stage 1 Intelligence in assisted level where there are no changes in the task, machine is able to learn thereby automating the task.
Stage 2 Intelligence in augmented level, where nature of task changes and information are passed from machine to human and from human to machine.
Stage 3 Intelligence in autonomous level, where the task nature changes with continuous learning by machines and automated decisions.

Intelligence in assisted level allows the repetitive process of automation with the routine manual task and cognitive task. More complex situations are handled by intelligence in augmented level which enhances the decision making by human. Lastly when the situation is learned enough by the machines such that decision taken by the machine is reliable for the human to trust then the intelligence is considered as autonomous intelligence. A variety of artificial tools are involved in the field of artificial intelligence. Classification of these tools is as follows:

- Tools of AI for personal usage.
- Tools of AI for business usage.
- Tools of AI for using in industry specific business.

6 Integration of Smart Environment and Robots

Integrating the capabilities of smart environment and robots which are also indicated as autonomous agents, in the framework of Internet of Things pave the way for Internet of Robotic Things. This conceptual framework is represented in pictorial form in Fig. 6. In this framework, smart environment indicates smart building, smart home, smart industry and smart city where automation is involved for performing the jobs in a smart way without human intervention (Vashi, 2011). In these applications, state of functions and processes involved in it are monitored continuously carried out in a controlled area which means maintaining environmental conditions such as temperature of the area using HVAC (Heating and Ventilation Air Conditioning) system or just to monitor the temperature using sensors.

Actuation can be carried out based on the parameters obtained from the sensors such as drives opening and closing window or switching on or off the air conditioner. In smart environment, the objective is to reduce power consumption where depending on the presence of human electric power is switched on or off. Even the electric appliances can be launched to operate during minimum power overload. Therefore, smart environment involves just the function of monitoring and sometime simple actuations that are performed only indoor as it has no agents for performing tough actions such as manipulators, robots, mobile robots, assistive robots, or service robots.

Integrating smart environment with such intelligent agents leads to Internet of Robotic Things which combines the functions of Robots in smart environment which expand their usage. Generally, roboticists focus on raising the autonomy of robots which requires enhanced sensors in robots and independent processing of data onboard allowing the robot to perform the task in an effective manner. Most often the fact is ignored that in a smart environment that is executed indoor, when some operations are executed by robots, we can even include several sensors such as magnetic sensors, Radio Frequency Identification (RFID), surveillance camera, routers, occupancy sensors, servers, smart phones, IR beacons, sonic beacons, computers.

This concept is considered in IoRT where both the functions of smart environment and robots are integrated for mutual benefits where monitoring is done by smart environment along with simple actuations using simple drives, integrated with robots which are able to perform complex task within the smart environment. Due to the process of integration, tasks are received by the robots from the smart factory or smart home where monitoring of the process is done based on which instructions are given to the robots to execute in the smart environment connected with sensors which leads to smart task such as navigation in a optimal way, avoidance of collision and effective interaction between human and robot. Hence, Internet of Robotic Things are advance level of Robots or IoT smart environment, which combines modern technologies such as wireless sensors, cloud computation, smart actuation, secured data, monitoring of smart environment, autonomy of decision, distributed networking, controlling by multi-agent, swarm, mapping and localization, interaction between human and robot, planning and control.

Baseline of IoT and Robotics—Sensors and Actuators

The two technologies that act as baseline in the field of Internet of Things and robotics are the sensors and actuators, the devices that make the environment to work in a smart way. Internet of Robotic Things can be implemented by these two crucial components with interfaces that are well defined such as identification and reaction in order to offer the functionalities of the platform of IoRT through the components of interaction. The building blocks of IoRT are the various sensors and actuators which function together to meet the goal of applications of IoRT. Usage of external building blocks is defined by Robotic Interaction Services which abstracts the service robot hardware system and the function of human-robot interaction (HRI). Calling of a function available in the robotic system such as functions available in an intelligent sensing system or service robot is called functional implementation. Implementation of services using a set of sensors and actuators is known as a robotic system.

Implementation of functions such as wheel control and face recognition depends mainly on the robotic hardware such as camera, Radar, microphone, Lidar which acts as sensors and actuators. The components that are involved in Human Robotic Interaction such as detection of person, identification of person are the functional elements in the logical form which are generally realized by sensors or other physical units fixed on the robot or in the smart environment. Main focus is on the scenarios of HRI, even though this standard is considered as a significant part for building applications that are deployed on devices as well on gateways. Potential inheritance is involved in robotic things for the process of variable and complex sensing and for the process of complex actuation when compared to the conventional system of robotics.

The field of robotic science and technology provides algorithm and methods that has to be used for simple sensors and sophisticated sensors as shown in Fig. 7 which includes inertial sensors such as compass, accelerometer and gyro, ranging sensors such as Radar, Sonar and Lidar and 3D

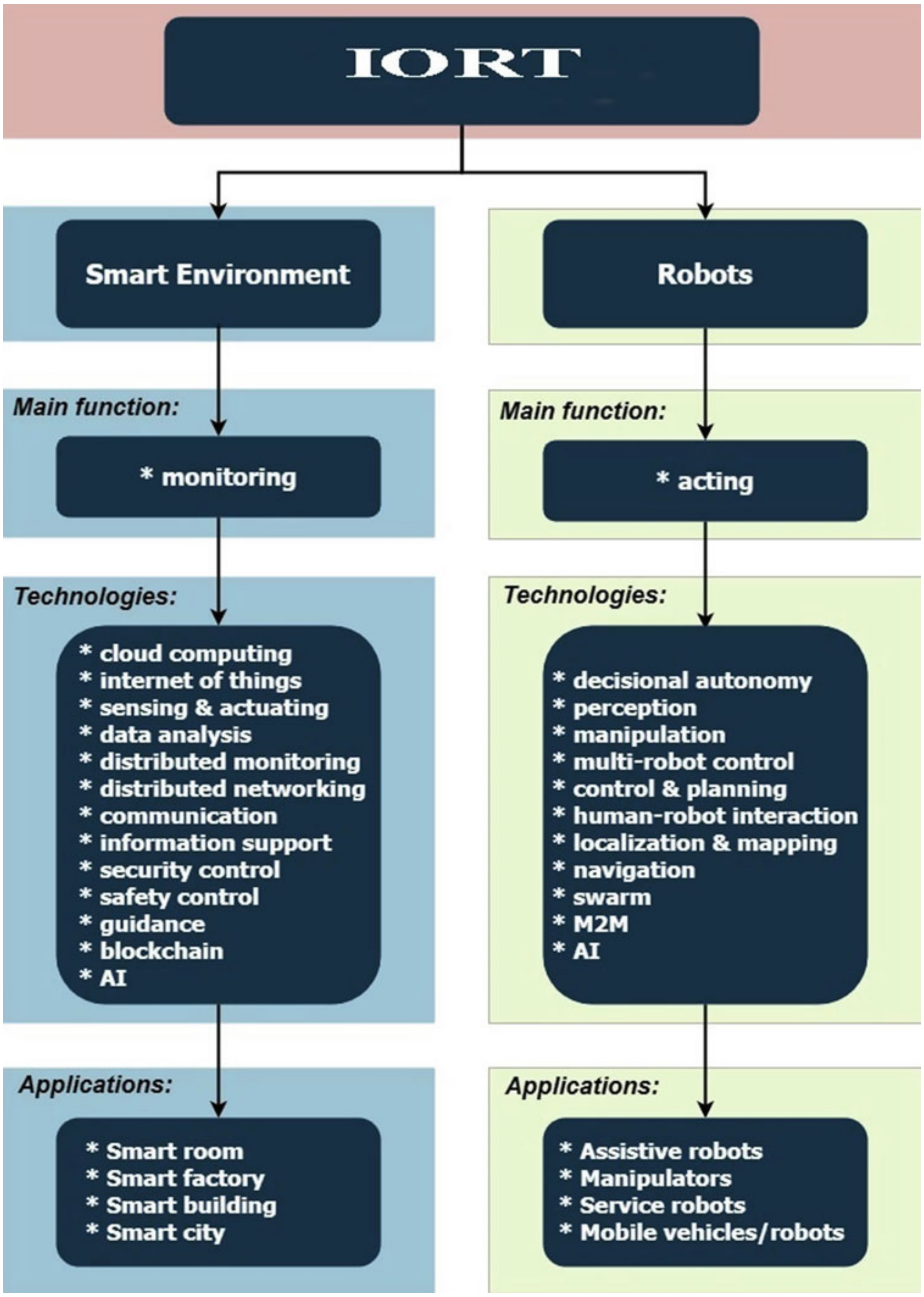


Fig. 6 Conceptual framework of internet of robotic things

sensors such as RGBD camera, 3D laser and other common sensors such as force sensors, microphones and cameras. Multiple or mobile robots collect data from the sensors by multiple techniques at multiple times such that this data can be combined together for a smart environment. Actually, modification of physical environment is considered as the unique feature of the robotic systems. A wide range of forms is taken by actuation from simple devices performing operation such as an automatic door to complex automation such as transportation and logistics by manipulation. Development of techniques of impressive range for actuation in the field of robotics is done which includes action execution by single robot or multiple robots and autonomous planning. Applications of IoRT are in requirement of low-cost imaging sensors based on CMOS technology which is based on laser active illumination which are larger in size for various environmental conditions in presence of fog, rain, dust, darkness, sunlight, etc.

Sensors involved in robotic system need to scan both the surface of the road where it needs to move which is the

Fig. 7 Sensors and actuators in robotic systems

horizontal projection and also needs to detect the object which is the vertical projection with higher accuracy and resolution. Sensors utilized in the current era provide the sensing information only in two dimensions or 2D which is then focused by sensor fusion for the representation of the 2D sensing data. Functions of IoRT for future applications require three-dimensional data such as 3D mapping and fusion of sensor data and actuation data. Hence, the robotic things have the requirement of an environment of 3D model which adapts itself for the new technologies of sensor to interpret highly accurate scene in order to collaborate with other robotic things. This is possible by optimizing the 3D representation in the smart environment which is a tradeoff between the optimal performance and demand of the resource.

In complex autonomous robotic things or autonomous vehicles, vision in 360 degrees is through LIDAR system due to the rotating mirror which scans in all directions to provide a view of all around. Accurate information about the surrounding environment is provided by the LIDAR system in 3D for enabling the quick making of decisions required for the autonomous robotic thing in self-driving mode. This is used after processing for identification of object, determination of motion vector, prediction of collision and strategies for avoidance of obstacle. For close-in control, operation is not effective with the usage of LIDAR systems; hence, it is necessary to equip the autonomous vehicles or autonomous robotic things with radars. The range of frequency at which radar operates is around 75–80 GHz has the characteristics of radio frequency propagation in order to provide resolution required for this case. Merits of this range of frequency are smaller size of radar devices and reduced amount of mutual interference due to lesser power of emission requirement. Hence for avoidance of collision in autonomous vehicles, promising technology is the radar scanning in environmental conditions with dust, smoke and other undesirable climatic conditions.

7 Computation Requirements

A huge amount of data is generated by Internet of Robotic Things which has to be processed to ensure efficient operation, also low computation power and data storage are available for the robots. Similar operation of data generation, processing, storage and actuation are carried out in IoT devices, hence there arises the need of increased computation power and data storage for the network of Internet of Robotic Things. Such resources are provided by the architectures of cloud and cloud computation.

Cloud Computation

A collaborative technology has emerged recently—synergy of IoT, robotics and cloud computing as Cloud Internet of robotics, where wireless networking is progressed along with the technologies of communication and large data storage (Siciliano & Khatib, 2008b). Following features are considered in the cloud computation for Internet of Robotic Things.

- Requirement of sensitivity and latency in the applications of IoRT but chances of generating high risk in life-related applications.
- Capability of autonomy and limited computational power of IoT in regard to the virtualized machines.
- Aggregating wide diversity of IoT devices along with heterogeneity of robotic devices is tedious to integrate to work together as a single system.

All the above risks can be overcome by performed by fog computation and edge computation.

Edge Computation

Multi-access edge computation or edge computation performs data processing where data creation is performed in the network as a substitute of warehouse which processes data in a centralized manner. Usage of edge devices enables the point of entry for the core networks. Distributed nodes such as edge or smart devices perform complete computation instead of environment with a centralized cloud.

Advantages of edge computing are obtained in the following cases:

Smart Vehicles with Autonomous Control

Smart vehicles must be compatible with self-driving option which can operate by itself without continuous connection with the cloud for processing data. But the smart vehicle is able to communicate with other vehicles in its surrounding based on the onboard processing.

Maintenance via Edge Computation

Detection of machines with high risk of breaking can be done by edge computation for fixing the predictive problem. Generation of alert is done by lowest latency within the line of sight of the machine.

Support by Fog Architecture

Computation for the distributed node model is referred as fog computation where computation is done by utilizing the edge devices acting as the terminals.

Fog Computation

Fog computation refers to the organizing process of edge computation in which the fog computing architecture indicates the operations involved between the resources of the cloud computation and end devices such as storage, computing and network services. Fog computation performs the extension of cloud computation till the edge of the network which is necessary for Internet of Things and other real-time applications. The fog network uses the resources available with local computer system instead of accessing the resources of the remote computer system thereby decreasing the latency of the network and increasing the performance level of the network in an efficient and powerful way.

Merits of Fog Computation

- Reduction of data transfer to cloud.
- Reduction of latency of the network.
- Allows network mobility.
- Conservation of bandwidth of the network.
- Improves response time of the system.

8 Cyber Security Issues

The complex problem involved in the field of Internet of Things and robotics obviously in Internet of Robotic Things is security, without which it leads to hacking of data from the communication link. Several reasons are there which causes the problem of cyber security in robotics which is discussed as follows:

- Cyber-attacks are due to communication done in an insecure way between human and robots which allows hacker to hack the link easily in no time.
- Issues related to authentication involve unauthorized accessing by the hackers to use the robotic systems from remote places without authenticated username and valid password.
- Lacking of encryption techniques leading to exposure of sensitive data by the hackers in a potential way.
- As the features of robots are programmable, if the hackers obtain the default configuration, then they can easily change the features of the robot.

Various problems involved in the cyber security of robotics are discussed along with the vulnerabilities and bugs that allow robots to get hacked from remote locations. Privacy and security solutions are to be implemented for preventing such hacking in robots. As automation systems and robotic systems rely on the software programmed and the data stored, cyber security is the requirement in such systems. Cloud computation and processing of big data is affected as accessing of datasets, libraries and maps are done which are associated with parallel grid computation with statistical analysis hence need to be considered under the problem of security.

Application of robotics based on IoT requires problem-solving capability, providing solutions for architectural problems, etc. Cyber security involves transfer of data and processing of data with the protocols of communication in an encrypted method. Another challenging problem of cloud computing is to provide cyber security for the IoT systems, as it involves connection of IoT devices through cloud where collection of data and communication is performed by cloud. In such condition, DDOS attack protection is an important part of security of the robotic system. Potential danger exists during interaction between human and robot due to the interference in communication which leads in variation of command to the robots. If the interface is not controlled by mechanism of authentication or encryption technique, then there are more possibilities of attacks by the hackers.

In mere future we can expect robots in every house such as robots acting as home assistants, household robots. This involves sensors, microphones and cameras for collecting data about the house members such as status of their health. Protection is required in such systems where confidentiality is needed to prevent accessing of data by unauthenticated entities or hackers.

9 Application Domains

Applications in the field of IoT and robotics can be classified in various ways, one among which is presented here:

(i) *Personal applications*

Collection of information from the sensors and using it for actuation is only by the individual who is the direct owner of the network.

(ii) *Industrial applications*

Data collection and actuation by IoT network are within a particular organization or company where the enterprise own the network.

(iii) *Utility-based applications*

IoT involved for the optimization of utilities on the whole such as smart monitoring of water network, smart monitoring of power utilization.

(iv) *Applications-based on mobility*

IoT-based applications involving mobility such as smart maintenance of urban traffic, smart automated logistics, smart loading and unloading.

The other method of classifying the application domains of IoT is as follows which is as shown in Fig. 8.

- Home automation.
- Automation in logistics.
- Health care.
- Smart transportation.
- Industrial automation.
- Agricultural automation.
- Smart city.
- Smart retail.

Benefits provided by Integrating IoT and Automation

Several benefits are provided by the integration of IoT with automation. Consider a smart hotel which operates based on IoT and automation; the benefits provided to the customer are as follows:

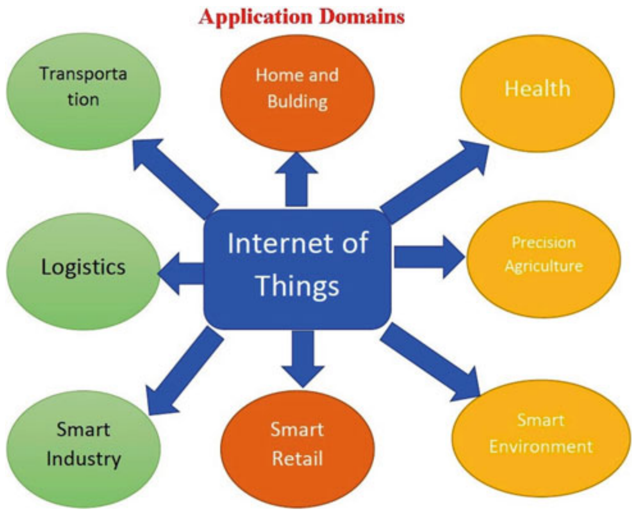


Fig. 8 Application domains of internet of things

- Rooms can be booked in a smart way online which allows cancelation at any time.
- Automatic temperature control of the room, where possibility to switch on or off-air conditioner from any place and any time.
- Customers can access the necessary information or status of the booked room such as human presence, temperature, humidity.
- Synchronization of data stored by the customer during the previous visit to the hotel.
- Online support to the customers to solve their problems in real time.

Several benefits provided by IoT in retail which are applicable to large companies also are as follows:

- Efficient operations are carried over as levels of inventories are tracked continuously by the sensors in real-time system.
- Customer stores are improved using smart mirrors by IoT which are of great help to retailers.
- Improvement in the relationship of retailer and supplier is obtained by IoT as frequent orders are placed by retailer automatically based on the tracking of inventories by the sensor system in real time.
- Shopping experience in a straightforward way is provided to the retailers where the customer data is scaled up including recommended shopping customization and portals for m-commerce and e-commerce.
- Demand can be forecasted using artificial intelligence which drives sales by maximizing the probability of stocked goods, assuring faster operations related to inventory.
- Customer data is analyzed using automation helping retailers to have better understanding of behavior such that adaptation is made in future transactions.
- "Chatbots" are operated using artificial intelligence by retailers that imitates interaction of sales executive and customer in order to meet the need of the customer in a best way.
- Computers are enabled to strategize information, observation and exploitation and to implement the process involved in the strategy.

Hence retailers need to follow certain strategies in order to extract maximum benefit from the integration of automation and IoT.

(i) New technologies have to be adopted to adapt to the competitive environment.
(ii) Consumer data has to be handled with care by setting up and following correct strategies.
(iii) Supplier relationship is redefined and reviewed in the play of supply and sales.

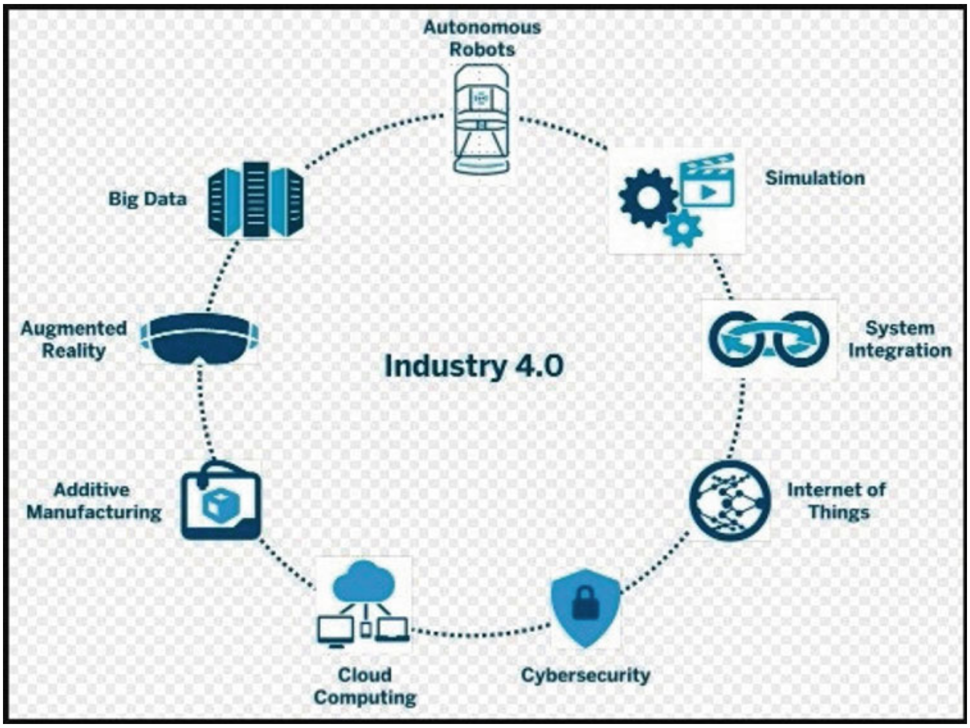
Several large retailers run their business based on IoT and automation such as Panasonic, Amazon Go, Smartrac, Walmart. Top industries which perform the business based on IoT and automation are as follows:

- Smart schools.
- Smart hospitals.
- Smart retailer shop.
- Smart industries with automated manufacturing.
- Smart logistics and transportation.
- Smart cinema halls.
- Smart vehicles.
- Smart financial support.
- Smart surveillance system.
- Smart buildings.

10 Internet of Robotic Things in Industries

Incorporation of Internet of Things and robotics is wider called as Internet of robotic Things which is mainly concerned with communication between machine to machine (M2M) such as robots and other smart devices where employment of data is driven to obtain the necessary outcomes. Robotic systems are smart devices which perform the monitoring process and data fusing from various resources for determining and execution of best actuation, for example, motion through an environment for manipulating objects in a

Fig. 9 Significant components of a smart industry



desired way. Applications that are performed potentially using IoRT are discussed as follows:

- Allocation of parking area for a car using robotic device which senses the empty locations in the parking stations.
- Decisions for operations in manufacturing industries are taken in collaboration of human and IoRT.
- Adaptability and flexibility is added to smart transportation by usage of IoRT.
- Domestic process of cleaning and assistance to elders by usage of IoRT.

Industrial automation is the major application using IoT, where the infrastructure of IoT is aided along with sensor network, communication through M2M, wireless communication for modernizing industrial automation in a complete manner. Many industries have adopted enhancements of IoT either in a small scale or large scale where process involved in industries are carried out through automation famously known as industrial automation Internet of Things (IAIoT).

IoRT integrated with IAIoT leads to Industrial Internet of Things (IIoT) which embraces the control systems involved in industries and manufacturing units. Assets of such smart industries are engines, robots, machines, sensor clouds, actuators, power grids etc. are involved in Industrial Internet of Things (IIoT). These assets work together as a large system for compromising the smart industries. Monitoring of data, collection of data, analysis of data, exchange of data, automatically change its state based on the data instantly can be performed by assets connected to the system. A practical scheme of classification with the security aspects of IIoT is discussed, as IIoT provides high efficiency at low cost, with quality products with less number of failures. The components of a smart factory are as shown in Fig. 9 whose important components include cloud computing, Internet of Things, Autonomous robots and Cyber security.

Interfacing between human and smart industry components is through chatbots which is easy to handle for providing interaction between robots and IoT in real time. In real time, there are various areas where robotics systems in integration with smart environment such as health care, smart logistics, home automation and smart logistics and transportation. Smart and software defined buildings can be introduced as a concept of smart environment where the buildings are programmable, with both hardware and software perform the sensing process such as presence sensing, face recognition, activity recognition and detection of emotion (Grieco, 2014; Ackerman, 2012). Different types of hardware components such as tracking sensors, occupancy detectors, positioning sensors integrate with the sensing functions of IoT.

Computation methods are used to process the raw data which is utilized as knowledge to the robots. Limited capabilities of sensing and memory of robots leads to the usage of SSDB, as a sensing system for the robots in order to increase the capability and autonomy of the robot. This makes the usage of robot as an actuator. Few applications of IoRT are discussed as follows:

Smart Home: Appropriate devices and sensors can be equipped for a smart home which interacts with the members of the home and with the robots involved for serving the human society in a better way. The services of smart home include, monitoring of nutrition with recommended meal, assisting children in doing their homework, monitoring of therapy for ill people. Robots that are programmed for doing service are designed such that they can help in household chore.

Smart Office: Equipping the smart office with devices and appropriate sensors, service can be provided in the visitor reception, conduction of official meetings and several other services for facilitating the workflow and for controlling the workflow. On the other hand, effective interaction can be done by programmed robots with the staffs and the visitors.

Smart Nursing Home: Special care can be given to patients round the clock and continuous monitoring is possible for the patient at lower cost due to the integration of IoRT. The service of activity announcement can announce the schedule every morning which included the events of the day or any other news or report, based on which the service robot is adapted for meeting the individual needs of the patient. Even the maintenance staff can be substituted partially by the involvement of IoRT and during necessity they can be called for help. Detection of elderly people can be done by smart environment, wandering and identified for disturbed behavior such that service robot assist these elder people. Several devices and sensors are connected in the patient's room in order to monitor the status of the patient, regulating medication and other controlled parameters of the room (Lastname et al., 2015).

Smart Industry: Automation is involved in the process of manufacturing and production which is monitored and controlled leading to quality products from the manufacturing unit. Environment of smart industry should be set up with equipment such that based on the emergency situation, environmental conditions must be adjusted. Loading process and unloading process can be performed in the industry by different type of robots such as stationary robot, mobile robot, autonomous robot and collaborative robot. The operation of production is done by welding robots, assembling robots which carry over the process of quality while machine control and equipment control can be done by mobile robots as shown in Fig. 10.

Fig. 10 Manufacturing robots in smart industry

11 Case Studies of Robotics and Automation

Synergy of robotics and automation in the field of IoT and IIoT has several real-time applications and case studies involved in different parts of the world which are listed as follows:

Fanuc Company: Minimizes Down Time of the Smart Factory Fanuc—famous robot maker has reduced the down time of the industries where this company makes use of robotics fixed with sensors with the analytics based on cloud. By this way prior information is obtained about failure of a robotic system or equipment involved in processing such that the down time of the industry is reduced. This effort is gifted by the zero-dynamic system of Fanuc. Beside this company several other companies implemented this system are as follows.

- Komatsu involved in heavy equipments for smart mining.
- Magna Steyr involved in manufacturing of smart automotives.
- Shell—innovator of smart oil field.

ABB Smart Robotics: This multinational robotic company has adopted Industrial Internet of Things (IIoT) to develop predictive maintenance system in an efficient way. The robots are monitored using the large number of sensors connected with the system and performs efficient maintenance by providing prior trigger for repairing before the breakage of the parts. Collaborative robotics of the company also depends on IoT. Human collaboration is possible by the company's YuMi model through the industrial protocols such as Device Net, Profibus and Ethernet.

KUKA Robotics: The IoT policy is extended throughout the factory such that KUKA was requested by Jeep for building a factory in order to produce one car body in 77 s. KUKA helped Jeep for building the company based on IoT connected with a private cloud, operating with hundred of robots such that 800 vehicles can be manufactured every day.

Home Automation: Home automation is based on Internet of Things which monitors and controls the parameters of the home. Intelligent preservation of energy is through the embedded system using PIC microcontroller. Home appliances such as fans and lights can be controlled and automated through the android interface using smart phone. The smart phone with android software does controlling and monitoring of various components which are connected to the micro web server through the module of Wi-Fi or LAN. The device status is tracked by the system itself.

Boeing Aviation Company: This multinational company of aviation has driven efficiency by deploying the technology of IIoT in the supply chains and industries for increasing the sensors connected in aircrafts. Service is the main concern of Boeing, the top provider of information in aviation.

Production of Oil Field: Optimization of oil production in fields is through IoT in the oil and gas company. Generally, sensors are used by this company for measuring the rate of oil extraction, pressure level in the well, temperature and other parameters of 21,000 oil wells. The readings are taken at a frequency of 90 per day with respect to the variable, such that 18,880 data is collected per day. The raw data obtained from IoT is converted into business data to obtain the tangible benefits which is employed by the company to analytically realize the opportunity and direct cost of analyzing the IoT data. Significant advancements of IoT in industries are analyzed. Similar automation can be implemented in water metering system in smart municipality where the water meters are mounted which can read and manually recorded. Also a truck manufacturer has connected sensors in about one lack trucks for maintenance to be done in predictive way. Scheduled repairing is carried out in the system automatically whenever necessary and the order for the spare parts are placed for repair automatically. In such system of maintenance data points of about 10,000 transmissions per day for every truck is carried out.

12 Robotic Applications Aided by IoT

Robotic systems aided with IoT finds wide range of applications where robots are included in manufacturing industries, health care, automobile factories, military field, exploration of deep underwater, exploration of space, rescue operation and operations concerned with security. A variety of problems are solved by the involvement of Industrial Internet of Things from monitoring of pressure and temperature to monitoring of electric grid and power consumption, etc. Applications of IoT include intrusion detection in railway stations, airports and seaports. Interaction between human and robot is efficient by pairing of IoT with artificial intelligence where possibility of understanding of natural language and perception is there. A key role is played by the Cloud Robotics for the robotic functions to get enabled such as sensing, mobility and manipulation. Robotic systems based on IoT finds applications even in the communication technology of shorter range, security assurance in environment that are smart and design of protocol. Best example of cloud robots is the autonomous car or driverless car which gets access through the Internet to the satellite image and map of the environment. Streaming data is exploited from its camera by the usage of sensor fusion and global positioning system as shown in Fig. 11 working integrated with three-dimensional sensors, accurate position is localized by a driverless car even within centimeter, as connection is also to an IoT platform.

Several benefits can be obtained in the field of transportation where every vehicle is in connection with IoT such that they travel in a smart environment fitted with all necessary sensors as shown in Fig. 12 Where traffic in real time is secured as transportation is done in an efficient way also maximum efficiency is attained in parking as the congestion is minimized. Operating cost is low as the operating data and early diagnosis reduces the cost of maintenance. As the vehicles connected to the IoT platform can talk to each other, there exist cooperation between the vehicles such that crashing is avoided leading to safe journey. In the applications aided by IoT, we must be aware that any device that communicates with the outside world can undergo cyber-attack which has to be avoided by special measures.

Home security is the important application of the robots aided with IoT and artificial intelligence. AppBot is an example of home security robot which is controlled by Wi-Fi through the Internet. Features provided by the robot are as follows:

- Remote control of appliances and their live view.
- To take snapshot and record video.
- Detection of motion and to track human who are in communication.
- Two-way communication.
- Accessing from anywhere is possible as connected to the router.
- Spontaneous capturing of intruders by the robot and providing immediate notification.

Now, we will focus on an industrial automation system aided with IoT and Artificial Intelligence which can take decisions in an intelligent way generating alerts and alarms whenever necessary. Remote sensing is enabled by Industrial Internet of Things by which the objects are controlled across the infrastructure of the network. This system is connected with variety of sensors which can sense temperature, humidity of the air, pressure level, vibration of the machines, intrusion, etc. in order to perceive the environment and the conditions of the objects in the industry. The

Fig. 11 Driveless car in an IoT platform

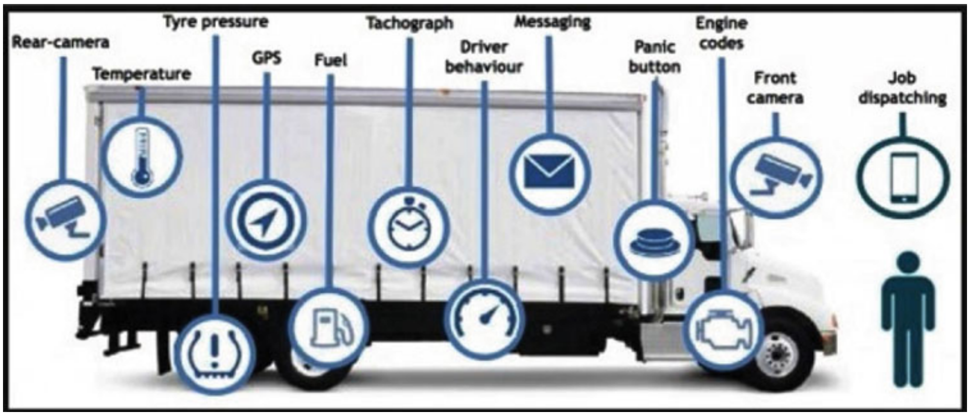


Fig. 12 Smart truck fitted with sensors

input to the smart device is in the form of analog signal which is compared with the threshold value already set by the programmer in order to check the condition of various parts of the machine. Whenever anomalous condition is found, notification is generated by special devices such as alarm or buzzer. These notifications are then immediately sent to the system administrator as an alert for taking proper measures to reset to normal operation as shown in Fig. 13.

The problem is resolved by the adequate steps taken with the aid of artificial intelligence based on the past experience and the data available in the data base for solving such problems and to avoid them in the future. Usage of cloud as

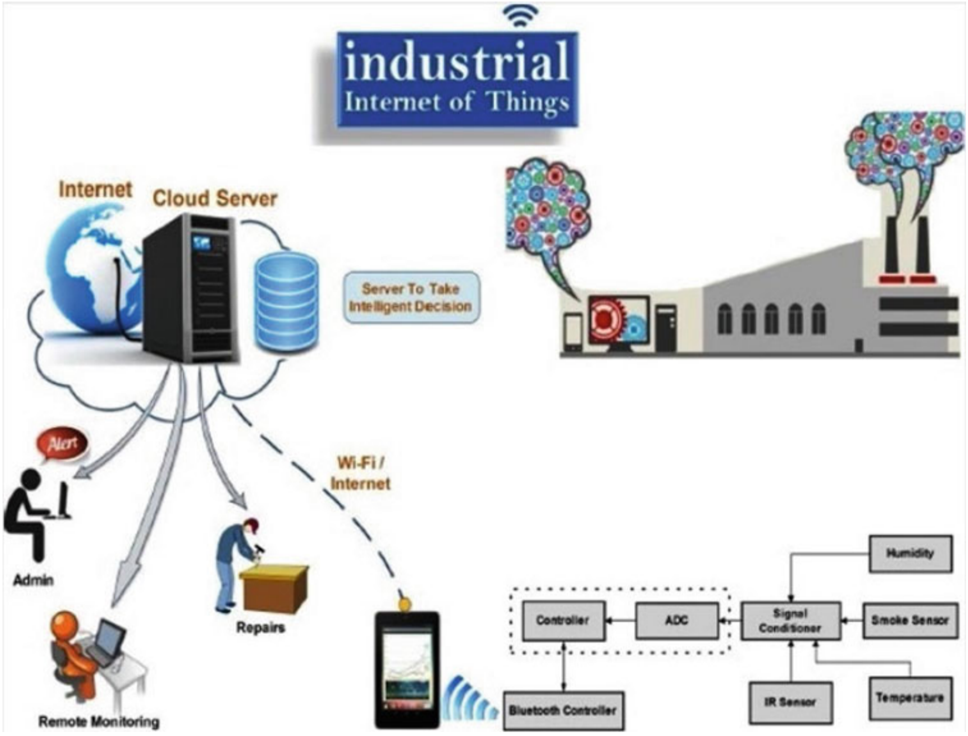


Fig. 13 Industrial automation aided with IoT and artificial intelligence

a scalable database is appropriate in such cases. Industrial Internet of Things integrated with cloud computing provides several computing services such as networking, database, storage, analytics, servers, software. Storage based on cloud provides the facility of storing data in remote database instead of storing of file in locally available storage device every time. Network sharing is fast with cloud computing rather than local networking.

13 Conclusion

The major field established with a multidisciplinary nature is the Internet of Things which promises for offering services of enormous value to the society. A great success is exhibited in complex in integration with the Artificial Intelligence with numerous applications in real time. A matured state has been reached by this field but still engineers and scientist are predicting that in future more advances will take place with benefits to the human society in an unimaginable way. In this chapter, a holistic overview of Internet of Things is compiled and its synergy with Artificial Intelligence in the field of robotics and smart environment to perform applications of industrial and home automation. Facility management is enabled successfully in industrial automation and IoT-based robotic automation where monitoring of production flow, control of inventory, management of supply chain, logistics and operation of robotic applications. Even though security provided by IoT has got considerable attention in the field from the beginning, the derived solution are not completely proved to be successful.

The biggest challenge in the field of Internet of Things and Industrial Internet of Things is the privacy and security. Designing is another problem for distributed IoT and also for many to many IoT which is also applicable for IIoT. This problem can be addressed by developing novel resource which is interrelated, interconnected and interdependent so that IoT provides collaborative and collective resource such that contribution is based on the individuals. Hence, implementation of IoT or IIoT is of high value in integration with Artificial Intelligence with its various applications in real time. The architectural concept of IoT-based robotics is proposed in this chapter which is termed as Internet of Robotic Things (IoRT) which is advanced networked robot of current cloud system. Robotic systems or robots under Internet of Robotic things can share, get connected, propagate the distributed resources of computation, context information, perform business activities and provide environmental data with other systems, accessing the knowledge and skills from others that are not self-learned, everything under the single framework of sophisticated architecture. This paves a way in the field of robotics which will lead to fascinating applications in future developments. Adaptation is allowed in the ecosystem of connection where deploying inexpensive robots are leverages by the technologies of heterogeneous environment which might be processing units, cloud services, communication network and various genres of devices. IoRT approach can benefit various fields with enormous developments which include navigation, grasping, etc. The architecture of IoRT combines the architecture of robotics and IoT together. Validation of the architecture shows emerging possibilities of novel techniques involving robotic systems and IoT processing units enabled by cloud computing. Future work can be extended by applying IoRT in various fields in smart environment in real time.

References

Ackerman. (2012). CMU's andy vision robot is in your store, doing your inventory. *IEEE Spectrum* [Online]. Available: https://spectrum.ieee.org/automaton/robotics/industrial-robots/cmu-andyvision-inventory-robot.

Anavangot, V., Menon, V. G., & Nayyar, A. (2018, November). Distributed big data analytics in the Internet of signals. In *2018 international conference on system modeling & advancement in research trends (SMART)* (pp. 73–77). IEEE.

Ando, N., Suehiro, T., Kitagaki, K., Kotoku, T., & Yoon, W.-K. (2005). RT-middleware: Distributed component middleware for RT (robot technology). In *Proceedings of IEEE/RSJ international conference on intelligent robots and system* (pp. 3933–3938).

Arai, T., Yasuda, M., Matsuhira, N. (2016). Development of a teleoperated robot arm system using RSNP: Precise tasks performed using a predictive display. In *Proceedings of 2016 13th international conference on ubiquitous robots and ambient intelligence (URAI)* (pp. 128–131).

Batth, R. S., Nayyar, A., & Nagpal, A. (2018, August). Internet of robotic things: Driving intelligent robotics of future-concept, architecture, applications and technologies. In *2018 4th international conference on computing sciences (ICCS)* (pp. 151–160). IEEE.

Campo, A., Gambi, D., Montanini, L., Perla, D., Raffaeli, L., & Spisante, S. (2016). MQTT in AAL systems for home monitoring of people with dementia. In *Proceedings of IEEE 27th annual international symposium personal, indoor, mobile radio communication (PIMRC)* (pp. 1–6).

Carpio, L. F. D., Di Marco, P., Skillermark, P., Chirikov, R., Lagergren, K., Amin, P. (2016). Comparison of 802.11ah and BLE for a home automation use case. In *Proceedings of IEEE 27th annuals international symposium personal, indoor, mobile radio communication (PIMRC)* (pp. 1–6).

Chattha, N. A. (2014). NFC—Vulnerabilities and defense. In *Proceedings of conference on information assurance cyber security (CIACS)* (pp. 35–38).

Chi, H. R., Tsang, K. F., Wu, C. K., & Hung, F. H. (2016). ZigBee based wireless sensor network in smart metering. In *Proceedings of 42nd annual conference on IEEE Indian electronics society* (pp. 5663–5666).

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Fernandes, J. L., Lopes, I. C., Rodrigues, J. J., & Ullah, S. (2013). Performance evaluation of RESTful Web services and AMQP protocol. In *Proceedings of IEEE 5th international conference on ubiquitous future network (ICUFN)* (pp. 810–815).

Fines, P., Christofylaki, E., Febvre, P., Khan, A. H. (2013). BGAN radio interface enhancements for SatCom-on-the-move. In *Proceedings of IEEE 77th 4G vehicle technology conference (VTC Spring)* (pp. 1–5).

Ford, S. (2016). ARM and the open internet of things, accessed. [Online]. Available: https://www.slideshare.net/slideshow/embed_code/45755086.

Furrer, J., Kamei, K., Sharma, C., Miyashita, T., & Hagita, N. (2012). UNR-PF: An open-source platform for cloud networked robotic services. In *Proceedings of IEEE/SICE international symposium systems integral (SII)* (pp. 945–950).

Gao, S., Gui, Z., & Wu, H. (2014). Extending WSDL for describing complex geodata in GIS service. In *Proceedings of IEEE 3rd international conference on agro-geoinformatics (agro-geoinformatics)* (pp. 1–6).

Giusto, D., Iera, A., Morabito, G., & Atzori, L. (Eds.). (2010). *The internet of things: 20th Tyrrhenian workshop on digital communications*. New York, NY, USA: Springer.

Grieco, et al. (2014). IoT-aided robotics applications: Technological implications, target domains and open issues. *Computer Communications, 54*(1), 32–47.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Henderson, K. Q., Latif, S. I., & Lazarou, G. Y. (2016). 'A microstrip line-fed multi-resonant slot antenna in the 4G/LTE band for smartphones. In *Proceedings of IEEE Military Communication Conference (MILCOM)* (pp. 208–212).

Hu, G, Tay, W. P., & Wen, Y. (2012). Cloud robotics: Architecture, challenges and applications. *IEEE Network, 26*(3), 21–28.

IEEE Society of robotics and automation's technical committee on networked robots [Online]. Available: https://www-users.cs.umn.edu/~isler/tc.

IoT Definition. (2012). Accessed on Jul. 4, 2012 [Online]. Available: https://www.itu.int/ITU-T/newslog/New+ITU+Standards+Define+The+Internet+Of+Things+And+Provide+The+Blueprints+For+Its+Development.

Kagaya. (2012). Strategy and efforts for robotics integration aiming at combining information and communications technology with robots. *NTT Technical Review, 10*(11), 1–7 [Online]. Available: https://www.nttreview.jp/archive/ntttechnical.php?contents=ntr201211fa10.

Kamei, K., Nishio, S., Hagita, N., Sato, M. (2012). Cloud networked robotics. *IEEE Network, 26*(3), 28–34.

Karjaluoto, H. (2006). An investigation of third generation (3G) mobile technologies and services. *Contemporary Management Research, 2* (2), 91–104.

Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015). A survey of research on cloud robotics and automation. *IEEE Transactions on Automation Science and Engineering, 12*(2), 398–409.

LLAP. (2020). Accessed on May 2020 [Online]. Available: https://openkontrol.org/llap/index.php/openkontrol/69-LLAP%20-%20Lightweight%20Local%20Automation%20Protocol.

Mizukawa et al. (2002). ORiN: Open robot interface for the network—The standard and unified network interface for industrial robot applications. In *Proceedings of IEEE 41st SICE annual conference (SICE)* (pp. 925–928).

Ma, X., Luo, W. (2008). The analysis of 6LowPAN technology. In *Proceedings of IEEE Pacific–Asia workshop computational intelligence and industrial application* (pp. 963–966). Wuhan, China.

Marcus, M. et al. (2015). Semi-autonomous domestic service robots: Evaluation of a user interface for remote manipulation and navigation with focus on effects of stereoscopic display. *International Journal of Society Robotics*, 7, 183–202.

Masirap, M., Amaran, M. H., Yussoff, Y. M., Rahman, R. A., & Hashim, H. (2016). Evaluation of reliable UDP-based transport protocols for internet of things (IoT). In *Proceedings of IEEE symposium computer applications and industrial electronics (ISCAIE)* (pp. 200–205).

Nayyar, A., Puri, V., & Le, D. N. (2017). Internet of nano things (IoNT): Next evolutionary step in nanotechnology. *Nanoscience and Nanotechnology, 7*(1), 4–8.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of things technologies for elderly health-care applications. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 217–243). Academic Press.

Peng, H. (2012). WIFI network information security analysis research. In *Proceedings of 2nd international conference on consumer electronics communication network (CECNet)* (pp. 2243–2245).

Pierleoni, P., Pernini, L., Belli, A., Palma, L., Maurizi, L., Valenti, S. (2016). Indoor localization system for AAL over IPv6 WSN. In *Proceedings of IEEE 27th annual international symposium personal indoor, mobile radio communication (PIMRC)* (pp. 1–7).

Postolache. (2016). Time-triggered CANopen implementation for networked embedded systems. In *Proceedings of IEEE 20th international conference on systems theory, control computing (ICSTCC)* (pp. 168–173).

Ray. (2016). Creating values out of internet of things: An indus- trial perspective. *Journal of Computer Network Communication, 2*, 1579460.

Saito, Y., Azumi, T., Kato, S., Nishio, N. (2016). Priority and synchronization support for ROS. In *Proceedings of IEEE 4th international conference on cyber-physical systems, networks, and applications (CPSNA)* (pp. 77–82).

Schütz, B., & Aschenbruck, N. (2016). Adding a network coding extension to CoAP for large resource transfer. In *Proceedings of IEEE 41st conference on local computer network. (LCN)* (pp. 715–722).

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Siciliano, B., & Khatib, O. (Eds.). (2008a). *Springer handbook of robotics*. Berlin, Germany: Springer.

Siciliano, B., Khatib, O. (2008b). Springer handbook of robotics. Berlin, Germany: Springer

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020a). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet, 12*(4), 61.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020b). Internet of things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth:, 2,* 191.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020c). Internet of things in pharma industry: possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Academic Press.

Smith, I. G. (2012). *The internet of things 2012: New Horizon*. Halifax, U.K.: IERC-Internet of Things European Research Cluster.

Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In *Handbook of Research on Big Data and the IoT* (pp. 379–405). IGI Global.

Stanik, Kao, O. (2016). A proposal for REST with XMPP as base protocol for intercloud communication. In *Proceedings of IEEE 7th international conference on information intelligence system and applications (IISA)* (pp. 1–6).

Tanwar, S. (2020). Fog data analytics for IoT applications—next generation process model with state-of-the-art technologies. *Studies in Big Data, 76,* 1–497.

Vashi. (2011). *Cloud robotics: An emerging research discipline*. Mälardalen University [Online]. Available: https://www.idt.mdh.se/kurser/ct3340/ht11/MINICONFERENCE/FinalPapers/ircse11_submission_20.pdf.

Wan, J., Tang, S., Yan, H., Li, D., Wang, S., Vasilakos, A. V. (2016). ‘Cloud robotics: Current status and open issues. *IEEE Access, 4*, 2797–2807.

Xue, W. K., Xiao, B. P., & Ma, L. (2016). Joint optimization of LORA and spares inventory with fuzzy parameters. In *Proceedings of IEEE international conference on industrial engineering and engineering management (IEEM)* (pp. 1640–1645).

Yarali, A., Ffahman, S. (2008). WiMAX broadband wireless access technology: Services, architecture and deployment models. In *Proceedings of Canadian conference electrical and computer engineering (CCECE)* (pp. 000077–000082).

Yassein, M. B., Mardini, W., & Khalil, A. (2016). Smart homes automation using Z-wave protocol. In *Proceedings of international conference on engineering MIS (ICEMIS)* (pp. 1–6).

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the- art and research challenges. *Journal of Internet Services Applications, 1*(1), 7–18.

Zhao, L., Meng, X., & Liu, F. (2016). Resonant frequency measurement of quartz crystal based on DDS and real-time peak searching. In *Proceedings of 6th international conference on instrument measurements computer communication control (IMCCC)* (pp. 513–516).

IoT in Smart Automation and Robotics with Streaming Analytical Challenges

R. Ganesh Babu, A. Karunakaran, G. Manikandan, S. Kalimuthu Kumar, and R. Selvameena

Abstract

The Internet of things (IoT) idea is advancing quickly and affecting new advancements in different application areas. For example, the Internet of mobile things (IoMT), autonomous Internet of things (An IoT), autonomous system of things (ASoT), Internet of autonomous things (IoAT), Internet of things clouds (IoT-C) and the Internet of robotic things (IoRT) that are regressing/progressing by utilizing IoT innovation. The IoRT speaks to new assembly challenges, and there should be tended to, in one surface the programmability and correspondence of various heterogeneous versatile/self-ruling/mechanical things for participating, their coordination, set up, trade of data, security, well-being and insurance. Advancements in IoT heterogeneous equal preparing/correspondence and dynamic frameworks dependent on parallelism and simultaneousness require new thoughts for coordinating the astute "gadgets", community robots (COBOTS) and keen on IoT appliance. Dynamic viability, identity mending, self-fix of assets, varying asset condition system and setting support IoT frameworks. Administration usage and reconciliation through IoT organize administration creation are of vital significance when original "intellectual gadgets" are turning out to be dynamic members in IoT applications.

Keywords

Internet of things (IoT) • Internet of robotic things (IoRT) • Intellectual gadgets • Dynamic frameworks • Community robots (COBOTS) • IoT frameworks

1 Introduction for IoT in Smart Automation and Robotics

The Internet of things (IoT) is striking with dynamic investigate territory, and simultaneously, mechanical technology is robust and set up a field with various applications (Akyildiz et al. 2006). Despite the way that for a long time, the two headings continued developing genuinely yet freely, indisputably present-day circumstances require a consolidation of the two controls and a joint effort from the organizations. With our work, we target developing this movement. It outlines the IoT and robotics developments alongside their blend towards the affirmation of Internet of robotics things (IoRT) (Akyildiz et al. 2011). We describe a couple of related thoughts, and we wisely mastermind them. This hypothetical edge is useful to examine and to recognize the top tier composing and how to arrive at a conspicuous determination into an exhaustive vision of things to come helpful vitality that requirements to meddle with IoT with robotics (Arslan 2007) unavoidably. The purpose of this document to give a predominant perception of the IoRT and recognize issues that justify analysing in the future. The articulation "web of things" (IoT) has starting late becomes popular to underscore the vision of an overall establishment that partners physical things/things, using a comparable

---

R. Ganesh Babu (✉)
Department of Electronics and Communication Engineering,
SRM TRP Engineering College, Trichy, India
e-mail: ganeshbaburajendran@gmail.com

A. Karunakaran
Department of Electronics and Communication Engineering,
Rajalakshmi Institute of Technology, Chennai, India
e-mail: karunakaran.a@ritchennai.edu.in

G. Manikandan
Department of Electronics and Communication Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India
e-mail: mrg.manikandan@gmail.com

S. Kalimuthu Kumar
Department of Biomedical Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, TN, India
e-mail: kali.12eee@gmail.com

R. Selvameena
Department of Computer Science and Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India
e-mail: rselvameena1989@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_7

Internet of Protocol, allowing them to pass on and share information.

The term IoT was created by Kevin Ashton in 1999 to suggest astoundingly conspicuous things/things and their virtual depictions in a web-like structure. As shown by inspector firm, 8.4 billion of things be related to the web in 2017; notwithstanding the workstations, PCs, tablets and phones. The amount of dynamic IoT devices is needed to create 10 billion by 2020 with 22 billion by 2025. IoT appliance is starting at now being used in contrasting spaces, for instance, clinical organizations field, healthy retail, customer help, astute homes, environmental checking and present-day web. The “Internet of robotic things” combines sensors with the content of robotized things, recognized due to their undeniable existence. Regardless, several difficulties are there to keep up this example.

1.1 Introduction of Automation and Robotics

Robotic technology is a field of the building that manages the structure and use of robots and the utilization of PC for their control and preparing. Robots are utilized in enterprises for accelerating the assembling cycle. They are additionally utilized in the field of atomic science, ocean investigation, overhauling of electric transmission signs and planning of bio-clinical supplies. Mechanical technology requires the use of PC coordinated assembling, mechanical designing, electrical building, organic mechanics and programming building.

Robotization and robotics engineering are the utilization of control frameworks and data advances to diminish the requirement for social work in the creation of merchandise and ventures. In the extent of industrialization, computerization is a stage past motorization.

A specialization in advanced mechanics designing may prompt potential vocation openings in assembling, exploration and building, horticulture, mining, atomic, power-plant maintenances and an assortment of different regions. Additionally, there is an incredible breadth for qualified specialists and analysts to connect themselves with various sections of R and D in mechanical technology. As the ongoing worldwide vocation pattern in mechanical technology proposes, fields as different as a medical procedure, current fighting and nanotechnology have enrolled an exceptional increment as of late in their interest for specialized experts and explores in mechanical technology.

1.2 Robots Roles

Today, these components are assisting with boosting robot appropriation in the sorts of use they as of now exceed expectations at today: monotonous, high-volume creation exercises. As the expense and unpredictability of mechanizing undertakings with robots go down, the sorts of organizations previously utilizing robots would utilize a more significant amount of them considerably. In the following five to ten years, in any case, we expect a more crucial change in the sorts of errands for which robots become both in fact and monetarily suitable (Exhibit 2). Here are a few models.

1.3 Automation Robotics Strategy

Robotization technique must line up with business and tasks system. As we have noted above, robotization can accomplish four key destinations: improving labourer security, decreasing costs, improving quality, and expanding adaptability. Progressed admirably, computerization may convey upgrades in every one of these regions. However, the equalization of advantages may fluctuate with various advancements and approaches. The correct equalization for any association relies upon its general tasks technique and its business objectives.

Computerization programmes must begin with away from the issue. It’s additionally significant this incorporates the reasons computerization is the correct arrangement. Each undertaking ought to have the option to distinguish where and how mechanization can offer upgrades and show how these enhancements connect to the organization’s general technique.

IoT is an empowering agent of the collaborative robots with a few papers contain just projected IoRT pedestal engineering ideas. All these examination work depends on automated frameworks to associate, share and disperse appropriated computational assets, business exercises, setting data and ecological information. Issues, for example, computational issues, advancement and security are frequently still open difficulties. Section 2 discusses the Internet of robotic things. A description of Internet of robotic things perception is seen in Sect. 3. Virtual and augmented realities are presented in Sects. 4 and 5 explains ML as enabler for adaptive mechanisms, Sect. 6 explains IoRT applications, and finally, the chapter concludes in Sect. 7.

2 Internets of the Robotic Things

The Internet of robotic things is concerned within the theoretical framework of IoT with the collaboration of smart world capabilities and automated operators (robots) (Doulamis 2018). In this, the idea is spoken to in a pictorial form as shown in Fig. 1. In this smart condition setting, we mean smart space, smart factory, smart building or smart city

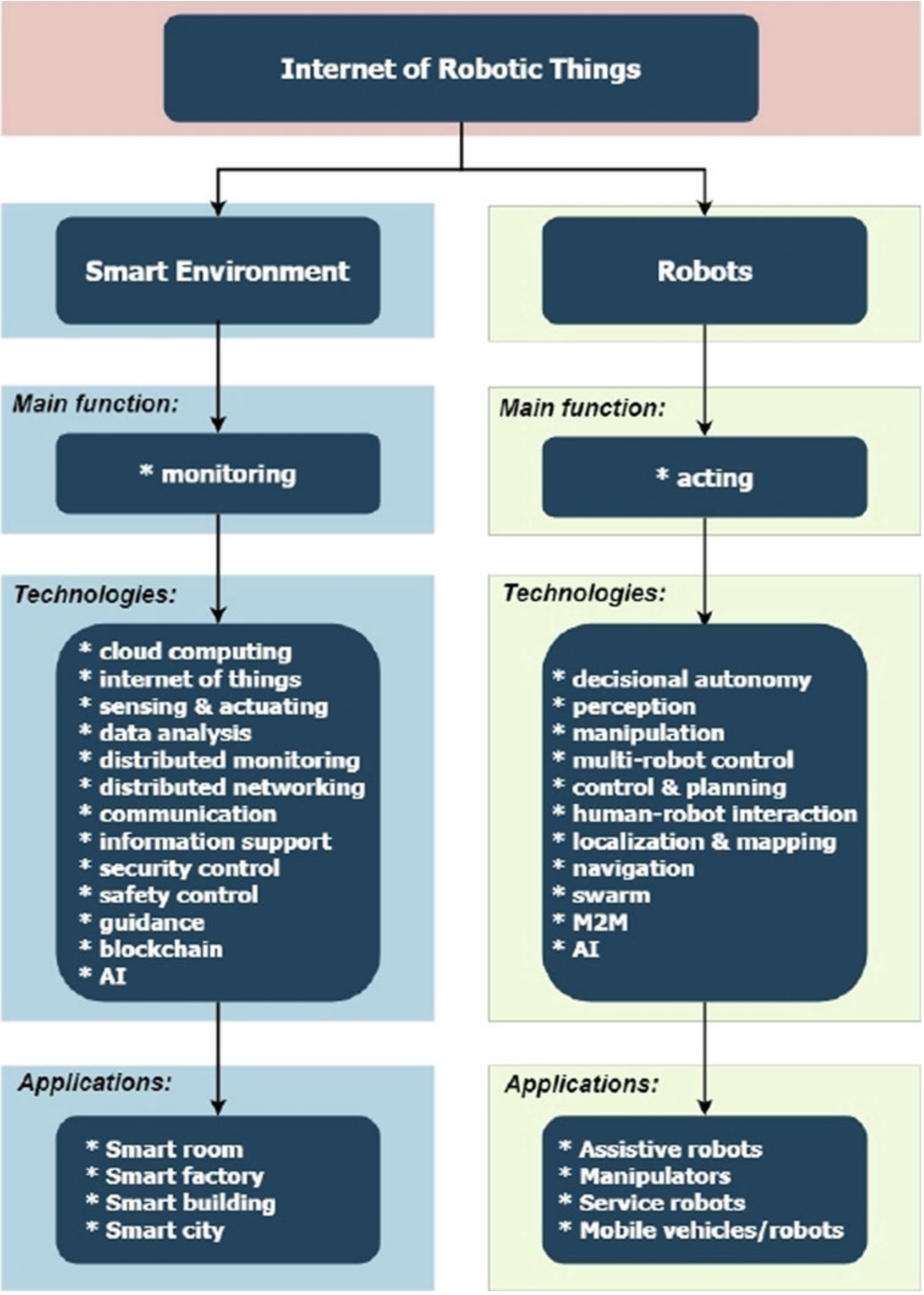


Fig. 1 Block scheme for the Internet of robotic things

applications. The fundamental capacity of these applications is the observing of states and procedures in a characterized controlling zone (Ekram and Bhargava 2007). Different capacities usually support the maintenance of such ideal environmental conditions such as temperature and air mugginess in space by using advanced heating ventilation air conditioning (HVAC) frameworks or by analysing states with specific sensors and devices.

Overseeing power utilization is likewise one of the targets at some point, for instance, by killing the electric force by controlling human nearness or propelling of family unit apparatuses, for example, a clothes washer, and so on when the everyday power taxes or power over-burdens are insignificant (Ganesh Babu 2016a, 2016b). Regardless of the accessibility of observing capacities and the necessary environment contain the operators to execute indoor behaviour (moving articles, playing out specific tasks or administrations, and so on.). Such specialists are robots, for example, assistive robots, controllers, administration robots and portable vehicles/robots.

The emergence of creative operators in the digital world ends the concept of the autonomous stuff Internet by combining the functionalities of the digital world and robotics, and by their potential effects. Current robotics much of the time centre just around expanding the degree of robot self-governance, improving the necessities for observation with robot sensors and locally available information preparing that ought to permit robots to perform errands autonomously. All the time they overlook the way the indoor condition of robots implement specific tasks, it loaded up and different sensors (RFID, inhabitance sensors and reconnaissance cameras, attractive sensors and IR/sonic reference points) and registering assets (PDAs, switches, PCs and servers). As per the IoRT idea, the two robots, whose functionalities expand by the keen condition assets, and the smart environment profit by shared combination, in which other than checking capacities and performing basic activities with necessary instruments, operators (robots) seem to execute complex tasks within the environment. Because of combination, robots get assignments from the environment likewise screens the advancement implementation task furthermore, offers clues to robots from the smart environment sensor arrange, for instance, for the ideal route, deterrent/impact evasion or successful human-robot connection (Ganesh Babu 2016c; Ganesh Babu and Amudha 2016d, 2016e, 2018a, 2018b). Accordingly, the IoRT is a further advanced degree of the permitting the current distributed computing, remote detecting and inciting, information investigation, confinement and mapping, route, multitude and human-robot collaboration—from the robot side (Fig. 1).

3 Internet of Robotic Things Perception

Computerized reasoning (AI), mechanical technology, AI and multitude advancements give the following period of improvement of IoT applications. Apply autonomy frameworks generally give the programmable measurement to machines. It intends to associate with severe and redundant work, just as a rich arrangement of advances to bode well their condition and follow-up on it, while computerized reasoning and AI permit/engage these machines to work utilizing dynamic and learning calculations as opposed to programming (Ganesh Babu and Amudha 2018c). The blend of these logical orders opens the improvements of self-sufficient programmable frameworks, joining mechanical autonomy and AI for structuring automated frameworks to be self-sufficient.

AI is a piece of a propelled condition of knowledge utilizing factual example acknowledgement, parametric/non-parametric calculations, neural systems, recommender frameworks, swarm innovations and so on to perform self-ruling undertakings. The utilization of correspondence focused on robots utilizing private correspondence and availability with sensors, and other system assets have been a developing and combining pattern in mechanical autonomy. It is associated with an interchanges system, for example, the Internet or LAN.

Self-governing robots and sensors trade the information through the system with the least human intercession. In such frameworks, the sensor organize expands the successful detecting scope of the robots, permitting them to speak with one another over significant distances to facilitate their action. The robots thus can send, fix, and keep up the sensor system to expand its life span and utility (Ganesh Babu et al. 2020).

Such strategies reflect specialized moves. It is described as disruption arrangement, reliability, clog, fixed or variable time delay, strength, aloofness of 100 IoRT sensing, range/force restrictions, organization, inclusion, protection, containment, incitement combination sensor and UI. New capacities emerge much of the time with the presentation of new equipment, programming and convention principles (Ganesh Babu et al. 2020).

The IoT advances and applications are getting significant changes in people's and society's perspective on how innovation and business work on the planet. Resident-driven IoT open conditions require handling new mechanical patterns and difficulties. In this unique circumstance, future improvements like IoT foundation and administrations meet. Mechanical and independent framework innovations to convey propelled usefulness, alongside novel applications and new plans of action and speculation openings require new IoT models, ideas and instruments to be incorporated away from any confining influence IoT stages structure and advancement.

The IoRT goes past organized and shared/cloud apply autonomy and incorporates heterogeneous savvy gadgets into circulated engineering of stages working equally in the cloud edge. IoRT deals with the numerous ways IoT today innovations and automated "gadgets" union to give progressed mechanical capacities. Empowering totalled IoT usefulness alongside novel applications by expansion. New business and venture openings in modern areas as well as in pretty much every part where mechanical help and IoT innovation and applications can be envisioned (home, city, structures, foundations and well-being).

Man-made brainpower (AI) methods empower IoT mechanical, intellectual frameworks to be coordinated with IoT applications consistently for making upgraded arrangements and for specific applications (Ganesh Babu et al. 2019; Karthika and Vidhya Saraswathi 2019, 2020). Subjective IoT innovations permit installing insight into frameworks and procedures. It permits organizations to expand productivity, find new business openings and to foresee

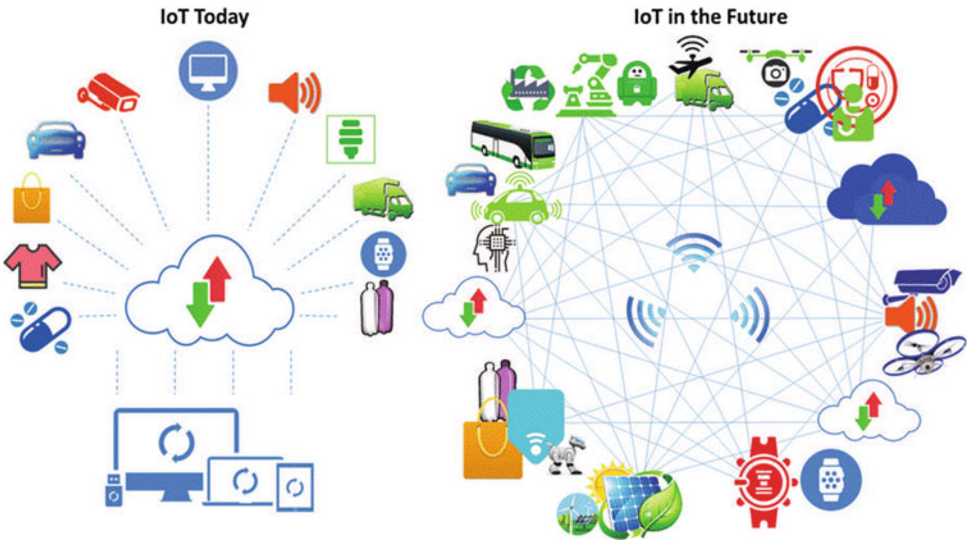


Fig. 2 From a brought together cloud to appropriated edge IoT stages and applications

dangers and dangers accordingly IoRT frameworks are better to get ready to address the different necessities in the normal more IoT complex condition as it is delineated (Karthika et al. 2019; Mekonnen et al. 2020; Mitola 2000; Mittal and Sangwan 2019; Nedumaran et al. 2017; Nedumaran et al. 2019).

The mix of cutting edge detecting/impelling, correspondence, neighbourhood and circulated preparing for IoT and mechanical autonomy arrangement suppliers, just as clients of their items. The idea empowers gauge attributes that can be summed up as follow.

Describe and depict the characteristics of mechanical self-sufficiency developments that remember them as an alternate, stand-out class of the IoT articles and differs amazingly from the ordinary cognizance of IoT edge centre points as direct, idle contraptions appear in Fig. 2. Uncover how the critical features of apply self-governance advancement, to be the explicit turn of events, convenience, control, understanding and independence, are updated by IoT perspective, and the IoT is developed via mechanized "objects" as "insightful" edge devices. Outline how IoT and mechanical innovation advancements join to oblige encompassing recognizing, enveloping information and encompassing limitation, which can be utilized by new classes of employments to pass on regard. IoT, personal processing and computerized reasoning advance reconciliation is a piece of the new improvements predicted for IoT applications in different keen situations.

3.1 Rising IoRT of Technologies

The Internet of things meaning states that, IoT is a robust worldwide system foundation with self-designing abilities. It depends on the standard and interoperable correspondence conventions. Here, physical and virtual "things" have characters, physical traits, utilize wise interfaces and are consistently coordinated into the data. The "things" are heterogeneous and have various degrees of unpredictability, detecting/activating, correspondence, handling, knowledge, versatility and are coordinated into various stages (Pouyanfar et al. 2018). The "automated" things are a class of unpredictable, canny and self-ruling that join techniques from mechanical autonomy and man-made reasoning. It is incorporated into a robust worldwide system framework with self-designing capacities. It is self-sufficient, self-learning conduct of associated automated things arranging frameworks that learn itself utilizing way and movement arranging and movement control to make benefits and give answers for explicit undertakings (Rondeau and Bostain 2009; Hailu and Nedumaran 2019; Tsai et al. 2015; Youssra and Sara 2018). In this unique situation, the IoT engineering incorporates the self-ruling framework design dependent on six principle qualities.

3.2 Applications with Improvements of the IoRT

Does not this look somewhat like the independent robots as we probably are aware of them, regardless of whether it's merely from motion pictures? Indeed, yes and no.

Considering that digital, physical IoT guarantee, it underlines the "physical" viewpoint more than is the situation in most IoT extends today where the fundamental spotlight is on "digital" part, as ABI Research puts it. Above all else how about we remind, it is still early days be that as it may, all the more significantly we should see use cases and what precisely is mean with control or control of a physical item and you will see we are a long way from those film robots.

Before doing so, we should likewise remind that we are talking about advanced mechanics in the more extensive sense, so not merely modern robots, regardless of whether that is the place we see some real undertakings. In any case, as per the prior referenced exploration, the development of the IoRT market is driven by, among other applications in web-based business (for example, at Amazon, more beneath). Yet additionally think robots in medical care, homegrown apparatuses (individual robots) and vehicles.

Time for specific models, activities and use cases on the Internet of robotic things. Communitarian robots and IoRT: FANUC Intelligent Edge Link and Drive FANUC, a prominent Japanese and worldwide dynamic producer of new and smart robots are in the Industrial Internet or Industry 4.0 space. An advertisements master of computerization for processing plants. To advance a system named 'FIELD' (FANUC Intelligent Edge Connection and Drive), they joined with Rockwell Automation, Chosen Networks and Cisco. It utilizes sensors, middleware, profound learning, edge processing and more to empower modern advanced mechanics gadgets that arrange and work together (read: act). Modern communitarian robots are one of the primary territories in IoRT.

3.3 Other IoRT Models: From Parking Area Robots to Cleaning Robots and Robotics

In a meeting in the summer of 2016, ABI research chief Philip Solis gave a couple of instances of likely utilization of the Internet of robotic things:

A mechanical gadget checks in a corporate parking garage, if a vehicle is approved to utilize that parcel and, if not, ready about it. He additionally refers to the case of Amazon Robotics' stockroom robotization satisfaction focus (here is our web-based business) where portable robots move canisters and beds and can arrange their developments (to stay away from mishaps). These are primarily still moderately early activities. You can envision applications in the personal robot space, as said additionally a developing marvel, whereby robots can make a genuine physical move by learning and consolidating sensor information, regardless of whether it is in garden upkeep, the backing of the old or cleaning. A frequently referenced model in such a manner is iRobot (cleaning machines).

4 Sensors and Actuators

The two examples of developments in IoT through mechanical advancement identified and interpreted throughout are sensor devices and sensors. They are reliably vital fragments for realized IoRT structures, both with specially represented interfaces (e.g., for recognition or reaction) also for providing these features through communication parts to the IoRT level. Not exactly equivalent to the IoT sensors and actuators make the supportive helpfulness all through the IoRT building squares.

The LIDAR framework gives exact 3D data on the general condition to empower for the self-driving self-ruling mechanical thing, which is prepared and utilized for object recognizable proof, movement vector assurance, impact forecast and hindrance evasion procedures.

4.1 Correspondence Technologies

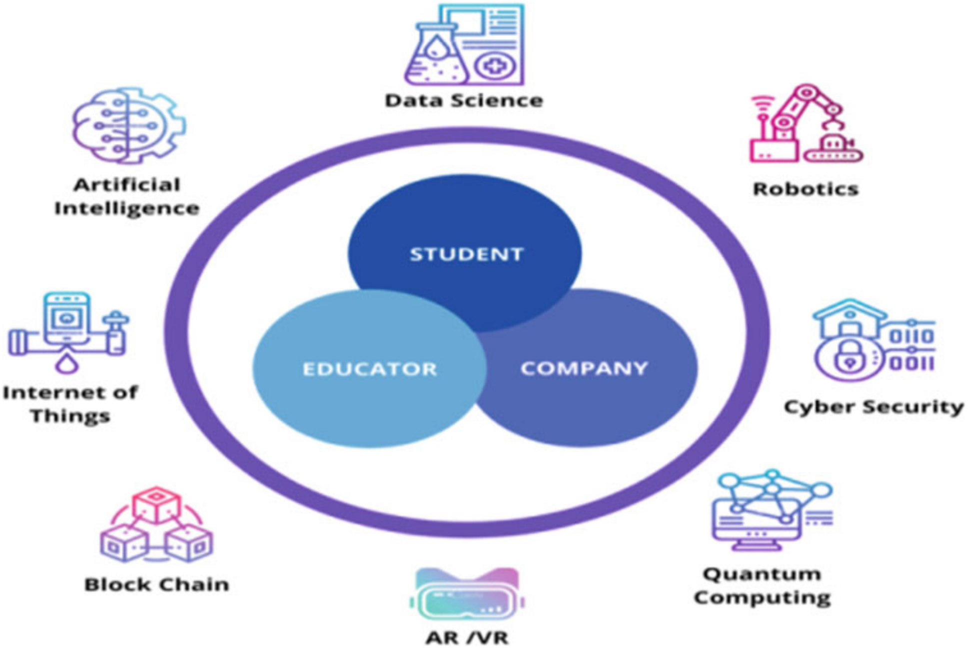
The correspondence engineering of IoRT needs new methodologies empowering shared continuous calculation. The trading of information streams (vital for 3D-mindfulness and vision frameworks) joined with internal correspondence, and edge registering to empower the virtualization of capacities on the current figuring motors, while empowering the convenience of such foundations in numerous spaces is shown in Fig. 3.

The correspondence framework and the IoRT outer correspondence should have the option to perform necessary time correspondence to guarantee impact counteraction gets conceivable, in this manner intensely lessening mishaps and crashes.

4.2 Preparing and Sensors/the Actuators of Data Fusion

Associated automated things can share the sensor information, meld and reason by being large about them. The portability and self-governance ability of automated acquires the issue of sensor combination IoT stages to an entirely new degree of intricacy and includes additional opportunities. Unpredictability is expanded due to the incredible sum and assortment of sensor information that automated things can give, and because the area of the detecting gadgets is not fixed and regularly is not know with conviction. Additional opportunities are empowered due to the capacity of automated things to self-sufficiently move to explicit areas to gather explicit tangible information, in light of the investigation of the right now access information and of the demonstrating and thinking objectives. The field of mechanical autonomy has built up a comprehensive exhibit of innovations for multi-robot sensor combination, just as for dynamic and objective coordinated observation. These procedures would empower IoRT frameworks to progressively and proactively gather broad scopes of information from the physical condition and to decipher them in semantically significant manners.

Fig. 3 Communication protocols used by different IoRT applications



5 Virtual and Augmented Realities

The increased reality devices permit subjective mechanical technology modellers to build, at ongoing, complex arranging situations for robots, wiping out the need to demonstrate the elements of both the robot and the actual condition as entire re-enactment conditions would require it. Such systems assemble a world model portrayal that fills in as ground truth for preparing and approving calculations for vision, movement arranging and control. The AR-based system is applied to assess the ability of the robot to design safe ways to objective areas in real open-air situations. At the same time, the arranging scene progressively changes, being enlarged by virtual items.

5.1 Voice Recognition, Voice Control

The informal boundary today focuses the talk bots with phone-engaged apps with little reach. The headway of IoRT appliance and the mechanized work joins a set of ending points that are associated with robotic things. Even the IoRT work progresses, supportive relationship between mechanical things rises, making the structure for new consistent and encompassing mechanized familiarity where computerized and individuals are collaborating.

In a unique situation, voice acknowledgement and voice the control of requires powerful techniques for wiping out the commotion by utilizing data the robot's movements and stances, because a sort of movement and signal creates nearly a similar example of clamour without fail. The nature of the mouthpiece is significant for programmed discourse acknowledgement to lessen the pickup of encompassing clamour. The voice acknowledgement control framework for robots can vigorously perceive voice by grown-ups and youngsters in boisterous conditions, where voice is caught utilizing small mouthpieces. To smother obstruction and clamour and to weaken resonation, the user utilizes a multi-channel framework comprising of an exception powerful summed up side-flap canceller strategy and a component-space commotion concealment measures.

5.2 Coordination

Brilliant conduct and participation among detecting and activating automated things are not yet considered in the spaces typically tended to with the arrangement and dynamic piece of web benefits in IoT stages. A middleware for prototyping of shrewd article conditions was taken into account. The creators reason that current endeavours are constrained in the administration. A subjective administration is required to satisfy IoT assumptions about setting mindfulness and client customized content administration. Methods for interoperability, reflection and aggregate knowledge should supplement the multi-operator the board for information reconciliation and combination and novel programming building strategies should be characterized.

The methodology is progressively broad, in that it thinks about profoundly heterogeneous gadgets, counting straightforward remote sensor arrange (WSN) hubs and smart objects. An expansion of this methodology, in light of imperative based arranging, was created in the FP7 ventures RUBICON and Robot Era. The methodology uses a web-based arranging and execution structure that joins unequivocal worldly thinking, and which is along these lines ready to consider various kinds of information and requirements standard for profoundly heterogeneous frameworks of automated gadgets working in open and dynamic situations.

5.3 Decentralized Cloud

The arrangement is the computational reaping, for example, offloading remaining computational task at hand utilizing decentralized cloud arrangements. It can work in two different ways. In the first place, from an asset obliged gadget to an edge cloud.

There is testing vitality execution exchange off between ready calculation and the expanded correspondence cost while considering system inertness. This methodology has been chiefly concentrated with regards to offloading video preparing outstanding tasks at hand from cell phones and keen glasses.

Comparable work is done with regards to the European tasks Robo Earth, what's more, follow-up Robo. Every one of these systems is mostly situated to permit the advancement of cloud-robot circulated applications and give no incorporation or usefulness to joining in the IoT. Besides, a self-coordination anxious mist is identified with the other way, for example, to move (computational or capacity) outstanding tasks at hand from the brought together cloud nearer to the endpoints (frequently the wellsprings of information).

5.4 Adjustment

Current IoT stages do not offer adequate help for versatility. It may be, the adjustment must be tended to for every application, and for the most part depends on pre-modified, static and fragile area information. Contrasted with sensor-based savvy questions, the quantity of settings wherein awesome automated things work is numerous. A few administrations are difficult to reach when associated with 4G). Additionally, non-mobile robots should be deftly reconfigured regarding programming and correspondence with different substances, for example, in deft Industry 4.0 assembling. Future mechanical things would be adaptable in their incitation abilities (for example, not restricted to solitary pre-customized usefulness). While the co-home of numerous applications expanding on similar sensor information is thoughtfully direct (could be viewed as the simple to resemble perusing activities of information in an OS), this case is not reasonable in incitation (which could be somewhat observed as "express" tasks).

A significant research question is how to boost application engineers to install their self-adjusting capacities of the IoRT biological system. One significant thought is that if applications are "assimilated" in the biological system, clients may not, at this point have the option to certify increased the value of special assistance, which may diminish their ability to pay (a negative impact for engineers).

6 ML as Enabler for Adaptive Mechanisms

The ML administration ought to not exclusively be appropriated, though it needs permitting installing insight on every hub of the IoRT, even at the edge of the system. These installed insights carry out the early combination and prescient information investigations. It produces a considerable level of low-level information/collected data. The gadget/sensor provides the crude information from which the application devours its assumptions. Accumulated expectations may become a contribution to another learning model situated on an alternate system hub where further forecasts and information combination tasks are performed, at last building an intelligent system of learning models performing gradual collections of the detected information.

Figure 4 shows a significant height portrayal of a circulated learning design to a system of insightful automated things, featuring of learning reproduction installed on the IoRT gadgets, with various computational, detecting and activation capacities. Figure 4 shows the measuring of learning models should be changed by the computational capacities of the facilitating gadget: a few gadgets may fill in as information suppliers for remote learning models. Remarkable processing offices, for example, cloud administrations, can be utilized to send more significant and increasingly complex learning models. The accumulate expectations from a few circulated learning models to give more significant level forecasts (for example, at the degree of territorial portals). Learning administration expectations should be given through particular interfaces to applications and IoRT administrations, executing unprecedented access approaches to the learning components.

From a logical point of view, the more extensive test is how to help applications and stage benefits in their self-adaptively all through circulated AI on IoT information. Fundamental difficulties in regards to interoperability should be tended to, for example, by what means can applications and administrations detail information handling demands for presently missing information and how these are converted into suitable sending systems.

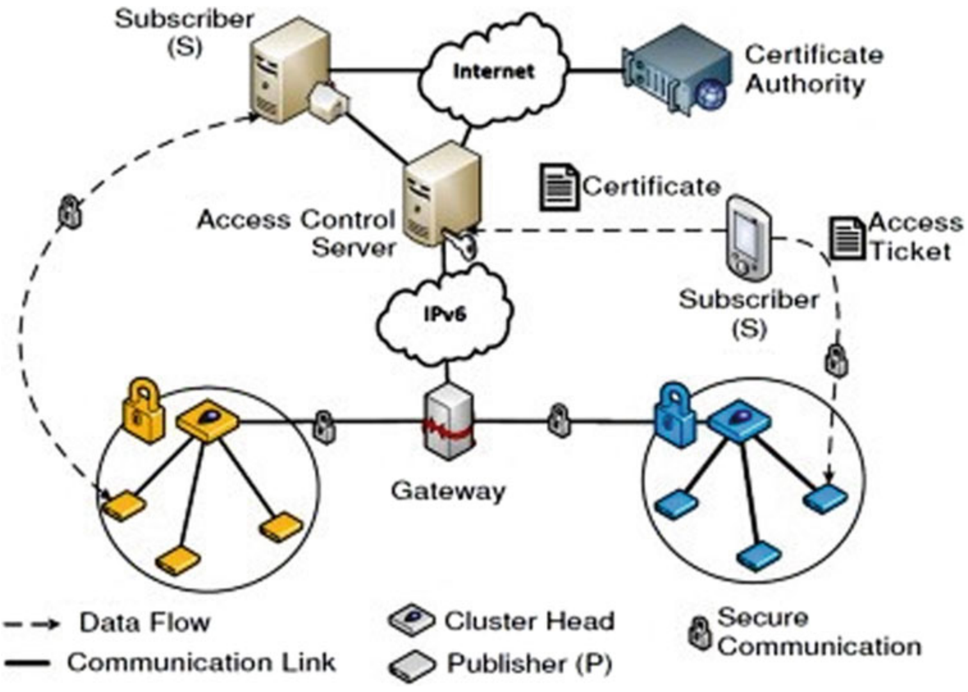


Fig. 4 Architecture of an IoRT learning system learning models

Resource believing also a different viewpoint to intentionally look at reserve use wants to be considered of deciding and submit ready blended learning, or marker, and must be monitored regularly (for example, to move a pointer effectively if facilities are inadequate or essential).

6.1 All the Way Operation and Information Technologies with Safety and Security of Framework

Certifiable checks that extend prosperity and protection are IoRT systems. The collaboration of frameworks with cameras/sensors and robotics used by essential dispatch organizations is also carried out. It fuses details from the relentless watch and scans for questionable/curious incidents while preserving the numerous dispatch organizations' in vital good ways.

The challenge of IoRT is to ensure that devices put stress on the insurance of individuals. Also, on the mystery and reliability of their data. Suppliers of IoRT empowered items and administrations ought to make convincing offers for information to be gathered and utilized, give straightforwardness into what information is utilized and how they are being utilized, and guarantee that the information is fittingly secured.

IoRT represents a test for associations that assemble information from automated frameworks and billions of gadgets that should have the option to shield information from unapproved gadgets. Yet, they need to manage new classes of hazard that having the Internet of robotic things associated with the Internet for all time can present. Expanding data innovation (IT) frameworks to new gadgets make a lot more open doors for possible penetrates must oversee. Besides, reach out past the unapproved arrival of data because possibly the reason for the potential physical mischief to people.

6.2 Square Chain

Square chain innovations, including circulated records and brilliant agreements, permit IoRT advances and applications to scale safely, join, consolidate and interface across different mechanical divisions. The innovation empowers a decentralized and robotized IoT framework that permits with trade information of administrations. The capacity square chains with other appropriated innovations to empower computerized and innovative machine to machine (mechanical things) systems are changing the structure, fabricating, circulation, coordination, retail, business and well-being applications. It affects pretty much every flexibly fastens from well-being to development and assembling (Fig. 5).

A blockchain-empowered union system is introduced in Fig. 6 to imagine the patterns as a durable stack. The base information assortment layer incorporates any sensor or equipment associated with the Internet accepting and transmitting the information.

The entire stack can be represented by a decentralized independent association constrained by human on-screen

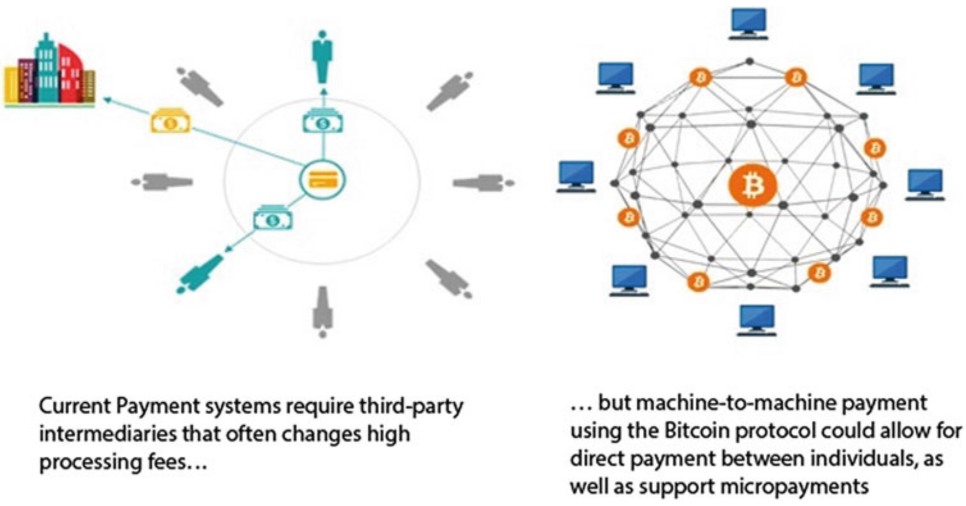


Fig. 5 Blockchain payment process—current versus bitcoin

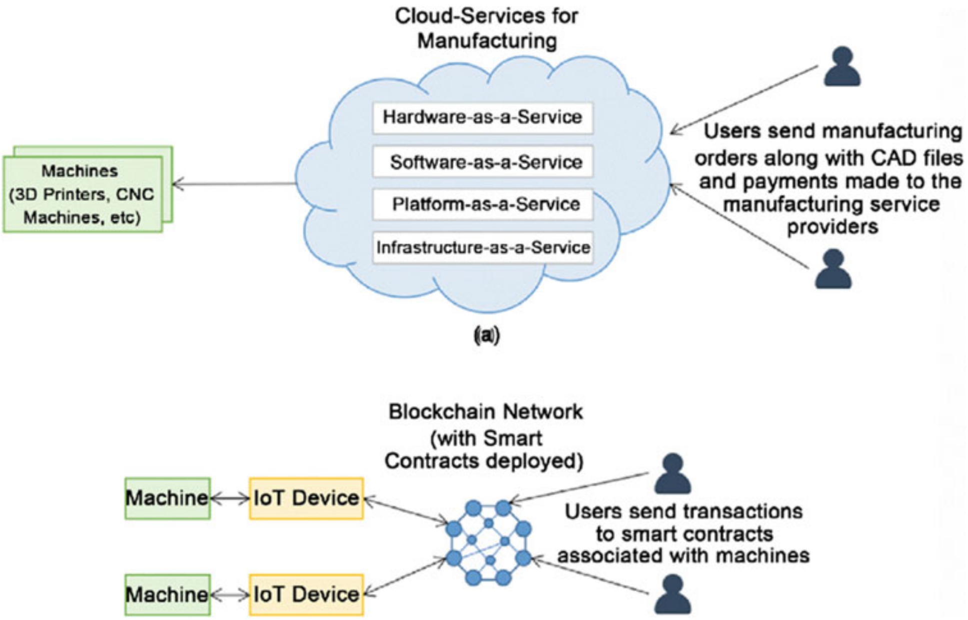


Fig. 6 Convergence framework for blockchain enabled

characters, or eventually, the whole stack overseen could establish a fake general knowledge (AGI). Blockchains, man-made consciousness, IoT, self-ruling mechanical technology, 3D printing and virtual and expanded the truth are on the whole merging to nearly upset existing ventures and make different markets and monetary models. The structure introduced should be incorporated as a feature of the IoT open stages design introduced.

Blockchain-based information commercial centre gives an approach to share. It adapts information, and new plans of action can be made with the goal that information suppliers can lease their information for a particular investigation, or timespan or even dependent on results.

As automatons and vehicles turn self-sufficient, they need an approach to share and execute information and critically, in systems, to arrange choices. Blockchains give an approach to accomplish bunch agreement all the more viably. The blockchain can use for various reason, as introduced in Fig. 7. Digitized renderings of conventional personality reports, for example, driver's licenses, identifications, birth endorsements, the government managed savings/Medicare cards, voter enlistment, and casting a ballot record. Access the executive's codes that give any character confined area, from site single sign-on to physical structures, brilliant vehicles and tagged areas, for example, occasion scenes or planes. A far-reaching perspective on clinical history that incorporates clinical and pharmaceutical records, doctor notes, wellness regimens and clinical gadget utilization information as an archive of important information, blockchain can furnish singular clients with command

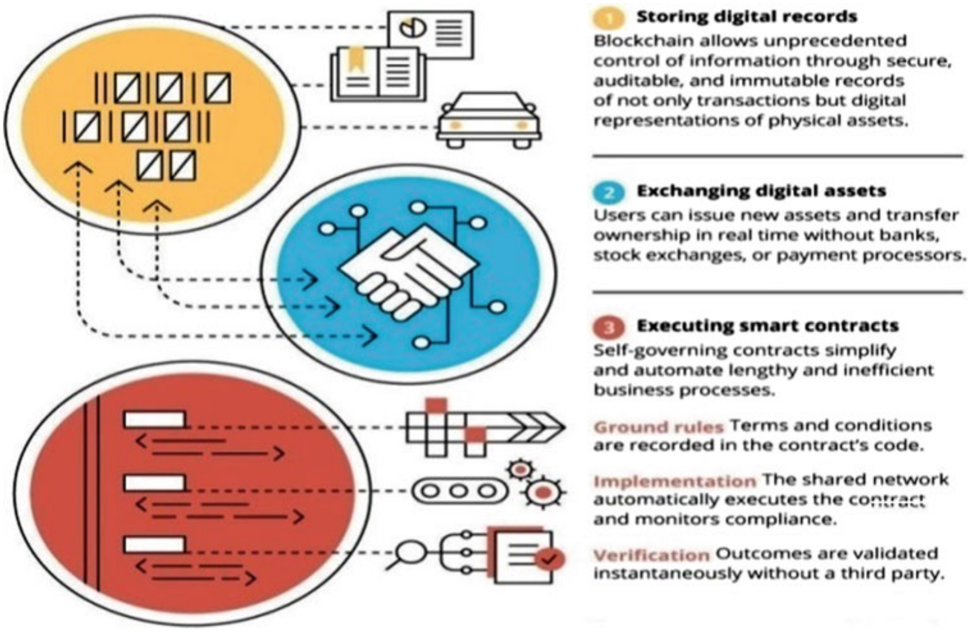


Fig. 7 Blockchain three levels

1 Storing digital records
Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions but digital representations of physical assets.

2 Exchanging digital assets
Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

3 Executing smart contracts
Self-governing contracts simplify and automate lengthy and inefficient business processes.

Ground rules Terms and conditions are recorded in the contract's code.

Implementation The shared network automatically executes the contract and monitors compliance.

Verification Outcomes are validated instantaneously without a third party.

over their advanced personalities. It can offer organizations a powerful method to separate data storehouses and lower information on the executives' costs.

Trade advanced resources without grinding: utilizing blockchain, gatherings can trade responsibility for resources progressively and, outstandingly, without all applications are requiring confided in computerized notorieties. The essential value-based model applies to P2P exchanges; blockchain might turn into a vehicle for confirming and clearing resource trades momentarily.

Execute keen agreements: not contracts in the legitimate sense, yet secluded, repeatable contents that broaden obstruct chains' utility from essentially tracking money related exchange passages to actualizing the terms of multiparty understandings consequently. Utilizing agreement conventions, a PC arrange builds up a grouping of activities from a shrewd agreement's code.

The security subject was not appropriately tended to by best in class inquire about for the most part because of the mind-boggling and heterogeneous attributes of automated multitude frameworks—robot self-rule, decentralized control, numerous individuals and aggregate rising conduct. Innovation, for example, blockchain can give not just a dependable distributed correspondence channel to crowd's specialists, but at the same time are an approach to defeat potential dangers, vulnerabilities and assaults. In the blockchain encryption, plot is introduced and strategies, for example, open key and advanced mark cryptography are viewed as acknowledged methods for not just creation exchanges utilizing hazardous and shared channels, yet demonstrating the character of explicit operators in a system. A couple of reciprocal keys, open and private, are made for every specialist to give these abilities, as introduced.

6.3 Hierarchical Interoperability

Propelled software-oriented architecture (SOA) principles, for example, remain dynamic in IoRT frameworks in administration coordination and movement. It is regardless of the possibility that an inexorably necessary job can defeat the ever-expanding uncertainty of the IoRT frameworks by equipping itself with the properties of self-designing, self-recovery, self-improvement and self-ensuring. A help orchestrator goes about as an assistant agent with extra help in observing capacities. In situations where recently chose administrations become inaccessible, or their exhibition drop or disappointment happens, the orchestrator might be utilized again to choose elective administrations as well as activating elective assistance structures. IoRT usage, the arrangement is typically performed on the ground-breaking backend, which organizes and coordinates the entire procedure and its members utilizing (web) administrations and message trade.

6.4 Semantic Interoperability

IoRT necessities regarding semantic interoperability involve stretching out existing ontologies to help the misuse of mechanical components, for example, abilities, administrations, shared procedures, typical assignments and objectives. Further building angles ought to be demonstrated to permit administration organization conveyed over numerous automated things, additionally to empower self-functionalities. It incorporates depicting every day, setting subordinate setups for asset sharing, arrangement and compromise among various cross-area administrations. These ontologies as of now characterize terms for impelling gadget and related ideas. In any case, those ontologies do not go further in the demonstrating of the interrelations of the activating gadget. It appears differently concerning the term of detecting gadget in those ontologies, which is connected to different ideas, as it is the customary core interest.

6.5 Syntactic Interoperability

IoRT frameworks involve upgrading leaving open APIs to empower key required by mechanical things of IoT stages, for example, disclosure, incitation, entrusting and lifecycle the board. One type of syntactic interoperability is computational gathering, for example, offloading of the remaining computational task at hand. It has been exhibited in two different ways: first, from an asset compelled gadget to an edge cloud. There is testing vitality execution exchange off between ready calculation and the expanded correspondence cost while considering system inertness. Furthermore, self-coordination tense mists are identified with the other way, for example, to move (computational or capacity) remaining tasks at hand unified cloud nearer to the edge (regularly the wellsprings of information). The permits to diminish inactivity of the control circles or to relieve the entrance data transfer capacity towards concentrated servers.

6.6 Stage Interoperability

It stays a test to help shut circle frameworks where sensor data is examined and utilized in situ and is vital for researching decentralized models to beat the inactivity and single purpose of disappointment issues related to unified ones. The related cooperation style, called a movement, is believed to be an increasingly appropriate approach to empower a consistent combination of supposed brilliant things or shrewd items inside general IoT frameworks. In any case, as opposed to on straightforward gadgets, for example, a gadget with constrained design alternatives, movement depends on operator like substances, for example, elements ready to execute business rationale and dynamic procedures and to cooperate among one another.

Also, the movement opens the topic of what conventions ought to be actualized by the savvy elements, as no norms yet exist. Regarding interoperability, it is imperative to refer crafted by the recently shaped. The gathering tends to a centre metaphysics that incorporates many terms commonly utilized in alongside approach received.

A few ontologies (Nayyar et al. 2017; Solanki and Nayyar 2019; Batth et al. 2018; Anavangot et al. 2018; Singh et al. 2020a; 2020b, 2020c; Dubey et al. 2020; Sehgal et al. 2020; Padikkapparambil et al. 2020; Tanwar 2020; Gupta et al. 2020) have been proposed for a few mechanical technology subdomains and salvage, independent driving, modern, clinical and individual/administration apply autonomy. In the space of self-governing robots, ontologies have been applied (Fig. 8).

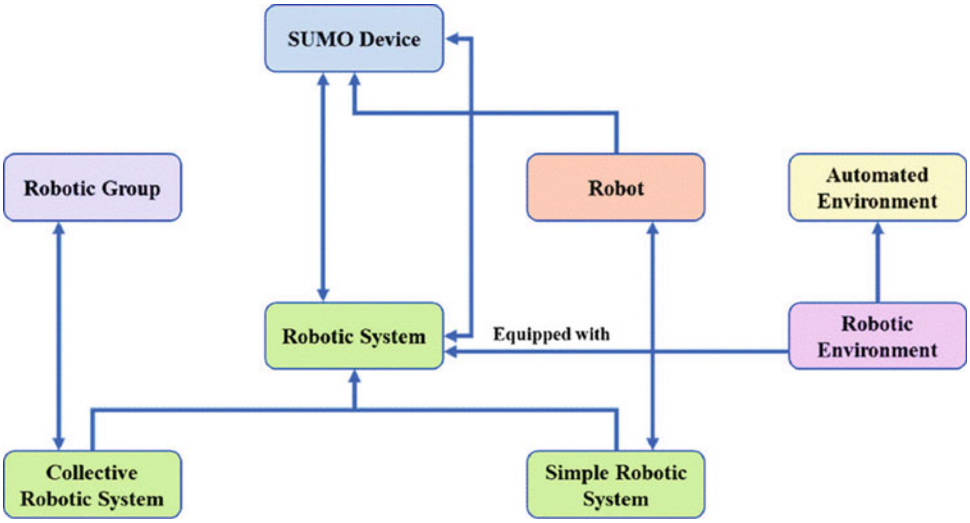


Fig. 8 Robotic system and its relations with a robot and robotic environment

7 IoRT Applications

7.1 Presentation

The exercises learnt in exploring system robot frameworks omnipresent mechanical autonomy, and automated ecologies are, robots are getting progressively increasingly self-governing. They are essentially progressively proficient and inherently increasingly viable on the off chance and are a piece of encompassing knowledge arrangements as a characteristic restrictive to have coordinated IoT conveyed frameworks with robotic frameworks. Licenses for mechanical technology and self-governing frameworks have expanded in the most recent decade. Other than robots utilized in industry and production line mechanization, administration mechanical autonomy for use in local, individual and medicinal services settings is the quickest developing area.

The accompanying segments give a short diagram of chances in chosen application spaces. Research enthusiasm for administration mechanical autonomy for help and prosperity has developed during the most recent couple of decades, especially as the outcome of segment changes.

Keeping up the right way of life and attempting to accomplish a condition of prosperity assists with improving the existing conditions and increment its toughness.

Administration mechanical technology could concentrate on early analysis and discovery of dangers to create counteraction programmes. Individual prosperity the executives' robots can offer types of assistance, likewise for individuals who are distant from everyone else separated from families. To specialist continuously and to decipher the enthusiastic condition of the client and as needs are communicated, the advancement of robots in various application territories introduced as the report from Yole Development in 2016.

7.2 Future Aspects Concerning the Internet of Robotic Things

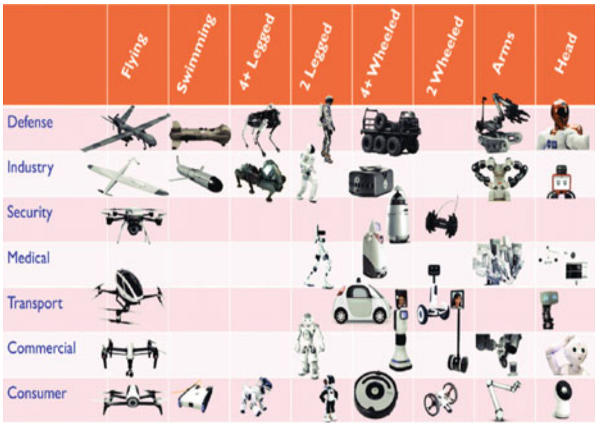
Mechanical systems (Solanki and Nayyar 2019) have acquired a few changes in different parts of the everyday living of people. Appropriation of robotics is finished by a few assembling businesses to play out a wide range of mind-boggling, critical and testing assignments like welding, product assembly, product testing, packaging, quality control and some more. Pre-programmed robotics have changed the essence of the industry more than ever with 100% precision and operational gauge of 24 × 7. With more headways, robotics got coordinated with organizing advancements which broadened their tasks in unstructured situations. As indicated by IEEE Society of Robotics and Automation-Technical Committee of Networked Robotics (Akyildiz et al. 2011), networked robot is characterized as, "a robotic gadget associated with a correspondence arrange like the Internet or LAN utilizing standard system conventions like TCP, UDP or 802.11". As indicated by the advisory group, there are two subclasses of networked robots: tele-worked: robots situated in far off areas and are constrained by people utilizing orders. Tele-worked advanced mechanics are generally used in exploration, instruction and overall population usage. Autonomous: robots coordinated with smart sensors working in the system and trading data. Sensor innovation expands the scope of the usefulness of robots to convey over longer separations to play out specific assignments in an exceptionally organized way. Web of things (IoT), soon by and large with different regions like artificial intelligence, machine learning, deep learning, augmented reality, cloud computing and swarm intelligence can change the substance of advanced mechanics by proposing cutting edge class of intelligent mechanical technology named as "web of robotic things (IoRT)".

7.3 Prescient and Preventive Maintenance

Machine upkeep for robots be IoT gear is very costly because the committed hardware and the important to execute that. For example, keeping up specific hardware may incorporate a "preventive upkeep agenda" which incorporates little watches that can fundamentally expand administration life. This data should be prepared by the support robot progressively or possibly in a couple of moments before the upkeep is planned to survey the best conditions to play out the support as shown in Table 1.

Numerous outer components, for example, climate and hardware are thought of; for instance, warming frameworks upkeep is regularly prescribed to be performed the winter to

Table 1 Application region and mobility development robots classification



forestall disappointments similarly HVAC is prescribed to be performed the most blazing season. It happens, however, in a perfect world, characterizes arranged support plans and conditions dependent on upkeep that assist with accomplishing certain degrees of profitable activity.

Robots, for the most part, are intended to protect and re-establish gear offering dependability by showing what are the parts that are required to be supplanted and in a like manner recognizing those ragged segments before they come up short. Upkeep incorporates preventive (fractional or complete) redesigns at determined periods, according to model, cleaning, oil, oil changes, parts substitution, check-ups, alterations, etc.

7.4 Independent Manufacturing

In this setting of expanding independence, innovations, for example, IoT and cloud foundation can be utilized to gather, investigate and envision ongoing creation execution markers, generally to illuminate existing streamlining forms. At the same time, results from multi-specialist frameworks and versatile middleware can give progressed proper coordination and correspondence conventions to facilitate the activities of various robots. Critical would be later on the capacity of robots to communicate and team up with human associates and eventually gain from these collaborators on the most proficient method to lead an errand.

Consequently, a significant subject is to make the cooperating of robots and people in the assembling procedure more secure to empower its heightening. Thus, robots must be empowered to foresee human conduct. The example created a universal reconciliation and disseminated correspondence system for the exchange of knowledge and organization of autonomous and human-robot cooperative operations. Metaphysics administrations are used to organize any single resources conceivable and connect them to a unified assignment coordinator for the higher-level organization.

7.5 Self-sufficient Home Application with Personal of Robots

Ordinary utilization of individual robots for help in household apparatuses, diversion and instruction. Coordinate innovation, residential environments speak to a significant spot. A few local help robots have been presented as consumer products for family activities, with a separate arrangement of floor cleaning robots, yard cutting robots, security robots, feline litter box robots and robot for cleaning up. Telepresence mechanical autonomy joins correspondence innovation with robots' observation capacities, in this manner permitting propelled cooperation abilities of people with remote situations. It permits individuals to screen patients or old individuals at home or in emergency clinics, to for all intents and purposes move and assess through far off conditions, and to take an interest in work gatherings.

Various researches recommend that applying autonomy coordination for instructive designs is a powerful instructing strategy that permits the advancement of understudy higher-request thinking abilities, for example, application, combination and assessment, just as cooperation, critical thinking, dynamic and logical examination. Additionally, mechanical autonomy utilized as instructive device assists understudies with building up the information and aptitudes required so as getting by information period of the twenty-first century.

Social legacies, films and retail condition speak to a novel and intriguing spot to incorporate innovation. Open and outside situations, as a spot for innovation, have an ever-increasing number of considerations later on, for the most part, because an ordinary life includes the capacity to be outside conditions. Research enthusiasm for administration applies autonomy for help and prosperity has developed during the most recent couple of decades, especially as the outcome of segment changes. Keeping up a reliable way of life and attempting to accomplish a state of prosperity assists with improving the existing conditions and increment its toughness.

Administration mechanical autonomy could concentrate on early finding and location of dangers to create avoidance programmes. In this manner, it is conceivable to utilize physical movement at home, or arranging a legitimate sustenance programme, in light of the client's needs. Individual prosperity the board robots can offer types of assistance additionally for individuals who are separated from everyone else or live segregated families. Individual robots speak to another age of robots that securely act and cooperate regarding complex natural conditions, and with moderately restricted vitality utilization and computational assets.

7.6 Medicinal Services Assistants, Elderly Support

The robot furnishes the client with a U.I. It goes about as a customized delegate of the administrations that the innovative condition offers. It has been appeared to build the client's acknowledgement of the innovation and offer included an incentive with administrations, for example, subjective incitement, treatment the executives, social incorporation/connectedness, instructing, fall dealing with and memory help. Consolidating IoT with AI and mechanical parts convey functional, measured, self-ruling and self-versatile IoRT frameworks has along these lines the possibility to supplement and improve the adequacy of existing consideration rehearses by giving robotized, nonstop appraisal of clients' bolster administrations can continually on top of clients' necessities.

8 Conclusion

IoT has highlights of reconnecting with various elements like applications, gadgets and individuals association, which gives the best answer for some application spaces. The mix of robotics, IoT and artificial intelligence brings about robots with higher ability to perform progressively complex assignments, self-rousingly or helping out people. With IoT stage, different robots can get effectively interconnected among them and with items and people, encouraging the capacity to move information to them without a human to PC or people to people's cooperation with the Internet of things as well as artificial intelligence. IoT includes highlights of reconnecting with different elements, such as apps, devices and the interaction of individuals, which offers the best response for specific spaces of operation. The combination of robotics, IoT and artificial intelligence produces robots with a higher capacity to increasingly perform complex tasks, self-rushing or helping people out. Only with IoT stage, different robots could also interconnect easily with each other and with objects as well as people, facilitating the ability to transfer information to them without people to PCs or people in cooperation with people. Thinking abilities originating from the utilization of AI, likewise misusing cloud assets, for instance, get helpful impacts terms of framework productivity and constancy, just as security for the client, and versatile physical and conduct human-robot connection/joint effort.

References

Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(13), 2127–2159.

Akyildiz, I. F., Lo, B. F., & Balakrishnan, R. (2011). Cooperative spectrum sensing in cognitive radio networks: A survey. *Physical Communication, 4*(1), 40–62.

Anavangot, V., Menon, V. G., & Nayyar, A. (2018, November). Distributed big data analytics in the Internet of signals. In *2018 International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 73–77). IEEE.

Arslan, H. (2007). *Cognitive radio, software defined radio, and adaptive wireless systems*. Springer.

Batth, R. S., Nayyar, A., & Nagpal, A. (2018, August). Internet of robotic things: Driving intelligent robotics of future-concept, architecture, applications and technologies. In *2018 4th International Conference on Computing Sciences (ICCS)* (pp. 151–160). IEEE.

Doulamis, N. (2018). Adaptable deep learning structures for object labeling/tracking under dynamic visual environments. *Multimedia Tools and Applications, 77*(8), 9651–9689.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Ekram, H., & Bhargava, V.K. (2007). *Cognitive wireless communications networks*. Springer Science & Business Media.

Ganesh Babu, R. (2016a). Helium's orbit Internet of Things (IoT) space. *International Journal of Computer Science and Wireless Security, 03*(02), 123–124.

Ganesh Babu, R. (2016b). Mismatch correction of analog to digital converter in digital communication receiver. *International Journal of Advanced Research Trends in Engineering and Technology, 3* (19), 264–268.

Ganesh Babu, R. (2016c). WIMAX capacity enchancements introducing full frequency reuse using MIMO techniques. *International Journal of Advanced Research in Biology Engineering Science and Technology, 2*(16), 1–7.

Ganesh Babu, R., & Amudha, V. (2016a). Cluster technique based channel sensing in cognitive radio networks. *International Journal of Control Theory and Applications, 9*(5), 207–213.

Ganesh Babu, R., & Amudha, V. (2016e). Spectrum sensing cluster techniques in cognitive radio networks. In *Proceedings of 4th International Conference on Recent Trends in Computer Science & Engineering, (ICRTCSE) in Association with Elsevier-Procedia Computer Science* (Vol. 87, pp. 258–263).

Ganesh Babu, R., & Amudha, V. (2018a). Allow a useful interference of authenticated secondary user in cognitive radio networks. *International Journal of Pure and Applied Mathematics, 119*(16), 3341–3354.

Ganesh Babu, R., & Amudha, V. (2018b). Comparative analysis of distributive firefly optimized spectrum sensing clustering techniques in cognitive radio networks. *Journal of Advanced Research in Dynamical and Control Systems, 10*(9), 1364–1373.

Ganesh Babu, R., & Amudha, V. (2018c). A survey on artificial intelligence techniques in cognitive radio networks. In *Proceedings of 1st International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS)in Association with Springer Advances in Intelligent Systems and Computing Series* (Vol. 755, pp. 99–110). Springer.

Ganesh Babu, R., Karthika, P., & Elangovan, K. (2019). Performance analysis for image security using SVM and ANN classification techniques. In *Proceedings of Third IEEE International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, RVS Technical Campus, Coimbatore, India (pp. 460–465).

Ganesh Babu, R., Amudha, V., & Karthika, P. (2020). Architectures and protocols for next-generation cognitive networking. In K. K. Singh, K. Cengiz, D. –N. Le & A. Singh (Eds.), *Machine learning and cognitive computing for mobile communications and wireless networks* (1st ed., pp. 155–177). Scrivener Publishing Partnering with Wiley. https://doi.org/10.1002/9781119640554.ch7.

Ganesh Babu, R., Karthika, P., & Aravinda Rajan, V. (2020). Secure IoT systems using raspberry pi machine learning artificial intelligence. In *Proceedings of Second International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT 2019) in Association with Lecture Notes on Data Engineering and Communications Technologies* (Vol. 44, pp. 797–805). Springer.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access, 8,* 24746–2477.

Hailu, Tegegn Ayalew, & Nedumaran, A. (2019). A survey on provisioning of quality of service (QoS) in MANET. *International Journal of Research and Advanced Development, 3*(2), 34–40.

Karthika, P., & Vidhya Saraswathi, P. (2019). Image security performance analysis for SVM and ANN classification techniques. *International Journal of Recent Technology and Engineering, 8* (4S2), 436–442.

Karthika, P., & Vidhya Saraswathi, P. (2020). Raspberry Pi: A tool for strategic machine learning security allocation in IoT. In N. Raju, M. Rajalakshmi, D. Goyal, S. Balamurugan, A. Elngar, B. Kesawn (Eds.), *Empowering artificial intelligence through machine learning* (pp. 133–141). Apple Academic press, CRC Press, Taylor & Francis Group.

Karthika, P., Ganesh Babu, R., & Nedumaran, A. (2019). Machine learning security allocation in IoT. In *Proceedings of IEEE International Conference on Intelligent Computing and Control Systems (ICICCS)*, Vaigai College of Engineering, Madurai, India (pp. 474–478).

Mekonnen, W. G., Hailu, T. A., Tamene, M., & Karthika, P. (2020). A dynamic efficient protocol secure for privacy preserving communication based VANET. In *Proceedings of Second International Conference on Computational Intelligence in Pattern Recognition (CIPR) in association with Advances in Intelligent Systems and Computing* (Vol. 1120, pp. 383–393). Springer.

Mitola, J. (2000). *Software radio architecture: Object-oriented approaches to wireless system engineering*. Wiley.

Mittal, S., & Sangwan, O. P. (2019). Big data analytics using machine learning techniques. In *Proceedings of 9th IEEE International Conference on Cloud Computing, Data Science ad Engineering (CONFLUENCE)*, Amity University, Noida, India (pp. 203–207).

Nayyar, A., Puri, V., & Le, D. N. (2017). Internet of nano things (IoNT): Next evolutionary step in nanotechnology. *Nanoscience and Nanotechnology, 7*(1), 4–8.

Nedumaran, A., Abdul Kerim, S., & Abdu, Tedros Salih. (2017). Advanced link state routing protocol approach for mobile ad-hoc networks. *International Journal for Scientific Research and Development, 5*(3), 516–519.

Nedumaran, A., Ganesh Babu, R., Mesmer Mesele Kass, & Karthika, P. (2019). Machine level classification using support vector machine. In *AIP Conference Proceedings of International Conference on Sustainable Manufacturing, Materials and Technologies (ICSMMT 2019),* Coimbatore, India (Vol. 2207(1), pp. 020013-1–020013-10).

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 217–243). Academic Press.

Pouyanfar, S., Sadiq, S., Iyengars, S. S., & Yan, Y. (2018). A survey on deep learning: Algorithms, techniques, and Applications. *ACM Computing Survey, 51*(5), 1–36.

Rondeau, T. W., & Bostain, C. W. (2009). *Artificial intelligence in wireless communication*. USA: Artech House.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IoT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020a). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet, 12*(4), 61.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020b). Internet of Things: from hype to reality. In *An industrial IoT approach for pharmaceutical industry growth* (Vol. 2, p. 191).

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020c). Internet of Things in pharma industry: Possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Academic Press.

Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In *Handbook of research on big data and the IoT* (pp. 379–405). IGI Global.

Tanwar, S. (2020). *Fog data analytics for IoT applications—Next generation process model with state-of-the-art technologies, Studies in big data* (Vol. 76, pp. 1–497). Springer International Publishing.

Tsai, C., Lai, C., Chao, H., & Vasilakos, A. V. (2015). Big data analytics: A survey. *Journal of Big Data, 2*(1), 1–32.

Youssra, R., & Sara, R. (2018). Big data and big data analytics: Concepts. *Types and Technologies, International Journal of Research and Engineering, 5*(9), 524–528.

Managing IoT and Cloud-Based Healthcare Record System Using Unique Identification Number to Promote Integrated Healthcare Delivery System: A Perspective from India

Ritam Dutta, Subhadip Chowdhury, and Krishna Kant Singh

Abstract

Being one of the most populous countries in the world, India has a healthcare delivery system that consists of both public and private concerns in four levels, i.e., Central, State, District, and Panchayati Raj level. The healthcare system of these levels has a separate database to store the patient history in large numbers and one has to carry his or her medical history in physical form for treatment in separate health centers. Each center has to send noticeable diseases to the health ministry. The objectives of this study are to search for a new area in our healthcare delivery system where digitalization can play a pivotal role, can mitigate any epidemic and pandemic disaster with ease, maintain single cloud-based medical records using single identity card anywhere in India, use biometrics or card number to access the medical history of the patient for a clinical, emergency, preventive, and mitigation using unique identity number (UID), viz. Aadhaar in India.

Keywords

IoT in health care • Unique identification number • Cloud-based computing system • Information retrieval • Monitoring and surveillance • Medical records

R. Dutta (✉)
Surendra Institute of Engineering and Management, MAKAUT, Siliguri, West Bengal, India
e-mail: ritamdutta1986@gmail.com

S. Chowdhury
DSMS Group of Institutions, Durgapur, West Bengal, India
e-mail: subha169@gmail.com

K. K. Singh
Department of Computer Science & Engineering,Faculty of Engineering & Technology, Jain (Deemed-to-be University), Bengaluru, India
e-mail: krishnaiitr2011@gmail.com

1 Introduction

India is a country with an approximate 1.31 billion population as of today, the latest Govt. of India Annual Census data shows in 2017 is estimated mid-year population 1,288,522,000 (Office of the Registrar General and Census Commissioner, India 2020). To cover this huge population, India has three layers of the healthcare system: 1. primary health care (PHC), 2. secondary level of health care, and 3. tertiary level of health care. Each level consists of a different model of healthcare delivery systems like subcenters, primary healthcare centers, subdivisional hospitals or community health centers, district-level hospitals as medical colleges, state-level hospital, and central-level hospitals like AIIMS. Medical records maintenance is necessary for every clinical center, be it outpatient or inpatient as per the Medical Council of India. Physicians have to maintain the record and for the notifiable disease, it has to be sent to the authority in due courses of time like STDs, and other communicable and occupational diseases. Definition of the medical record as per G. D. Mogli is as 'Medical record can be defined as an orderly written document encompassing the patient's identification data, health history, physical examination findings, laboratory reports, diagnosis, treatment, length of hospital stray, results of care, and future course of action' (Mogli 2006).

For this huge population, keeping the records in physical form is a mammoth task. For every medical center, medical record-keeping not only takes cost, time, and manpower requirements but also maintenance of the records is essential. Medical records are a legal document as it is evidence as per Indian Penal Code, document for insurance, workmen's compensation, personal injury suits, malpractice suits, probate case, notification of birth and death, criminal cases, medical reports and certificates, identification of the patient, etc (Mogli 2006).

The medical record is essential to store the patient's clinical history. Medical history is very vital for the treatment path. Now first let us understand why a patient's medical history is important. It consists of patient

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*, Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_8

identification number exclusive to the medical center where it generated patient's name, address, occupational data, gender, age, marital status, and some vital statistics primarily. Then the history consists of any previous illness, medications, diagnosis, surgery history, implantation history, known allergies, the prevalence of any disease, co-morbidity, immunization records, hospitalization records, etc. A proper maintained medical history not only helpful for the planning of future diagnosis and treatment but prevention against genetic diseases can be concluded. Even preventive actions can be taken for future generations from parent's medical history.

Now, medical records are important for a hospital or clinical establishments to be maintained and stores for a certain period. Not only past records but the chronologically maintaining of the present records of diagnosis and treatment is equally important. It not only a source to track the patient's improvement but also prevents any errors by different departments and physicians. A proper updated record facilitates the physician to check the progress, detect any anomalies, refer another specialist for further treatment or opinion, reduce the time and cost to prevent a repetition of the diagnosis tests, prevent an overdose of drugs or missing medications, and many more. Systematic proper medical records are essential in every case.

Digital India initiative by the Government of India, Ministry of Electronics and Information Technology and Finance Ministry was started on ^{t} July 1, 2015 (Digital India 2020). Through this initiative, India targets to digitalize all the aspects of the modern world from e-governance, e-banking, e-commerce to e-health care. From geo-informatics to COVID-19 protection and help app development, and socially responsible artificial intelligence applications are added to a new crown on India. Now India is a member of the Global Partnership on Artificial Intelligence (GPAI). Through this initiative, India takes the challenges of the e-healthcare initiative through different app-based and online services. A patient can book outpatient-based services or can book doctors through official Web sites of government hospitals. India develops successfully Aarogya Setu app for the public to help themselves in the COVID-19 situation (AarogyaSetu App 2020). Through digital India, government joining different identity numbers in one unique identification number (UID). Government links PAN with Aadhaar number, all the telephonic contact numbers to it, all the banking services and payment system to UID and many more like voter card. This UID will be one single identification number to access different government facilities and subsidies. Here, the importance of UID has infinite possibilities because India has a total 1.3 billion population with 1.23 billion Aadhaar card facility, 1.21 billion mobile phone users with 446 million smartphones, and 560 million Internet users as per 2018 data (Bureau 2019). Digital India initiative launches the DigiLocker system where all the important documents can be saved and accessed anywhere in softcopy form by any Indian who opted for the services (Digilocker services 2020). It will reduce the requirement to carry the physical document thus prevent damage or loss of the documents. Now under the Digital India initiative, the government introduces e-hospital services for central, state, autonomous, cooperative hospitals on the cloud through software as a service (SaaS) (E-hospital cloud 2020). This hospital information system connected all the departments like patient booking, services, blood bank, medical records, etc (Vikaspedia definition 2020). Through Aadhaar card and linked phone number, the patient can book and avail of the facility. UID Aadhaar card has some unique facility as it saves biometric data of the person and can be identified easily in any mishap. Another system tracks mother and child health, from the pregnancy to the immunization of the child developed by the digital India initiative for the Ministry of Health and Family Welfare (National Rural Health Mission, Mother, and Child Tracker 2020). All of the systems help to develop the primary base for this study on IoT and cloud-based medical record system which can be accessed through UID.

2 Use of IoT and Cloud-Based System in Health Care

The Internet of things (IoT) word was first coined by Kevin Ashton in 1999. He describes IoT as the Internet is connected to the physical world via ubiquitous sensors (Cole 2018). Here, the interrelating computing devices set up an ecosystem to generate and send data to each other via unique identifiers without any human-to-human or human-to-machine interactions (Internet of Things 2020). It is forecasted that IoT technology will reach 25–27 billion units by 2020–2021 (Gartner 2014). IoT has many technological advancements and some limitations too. The technology is always volatile and lots of ambiguity are there to use different platforms of IoT in this ever-changing environment. The platform for IoT thus has many opportunities to connect different machine and computing platform to produce a single ecosystem that can symmetry the whole system. This is used to control the objective of the system in the most efficient manner. The use of IoT in the industry has many varieties like using wireless sensor networks (WSN) (White and Cheong 2012)), radio frequency identification (RFID) (Amendola et al. 2014), and many real-time applications and sensors to promote artificial intelligence and neural network in the business, health care, and other areas.

The cloud-based computing method is used to store and access data over the Internet, and one can access the data any time from a device like Gmail where one can store the data over Google Drive and access it anywhere from a device through the Gmail application (Dell Technology 2020). Cloud-based services can facilitate different day-to-day operations from storing and retrieving data securely where there are no needs to store the data in a hard drive, online video streaming, social media networking, etc., through natural language processing and artificial intelligence (Ranger 2018). It can be done by mostly three techniques like infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) (Ranger 2018) where SaaS is used in most of the services to provide end users service irrespective of app or Web browsers or hardware. PaaS may use for developing middleware, database management, operating system, etc. IaaS serves as fundamental building blocks (Ranger 2018) for physical or virtual servers, storage and networking which can be provided rent or free access basis.

2.1 Healthcare Applications by IoT

In recent years, many healthcare applications that use the IoT system are working throughout the world. For example, different systems like community health care, adverse drug reaction (ADR), wearable device access (WDA), semantic medical access (SMA), indirect emergency health care (EMH), embedded gateway configuration (EGC), embedded context prediction (ECP), ambient-assisted living (AAL), Internet of m-health things (m-IoT), etc (Islam et al. 2015). These systems help the healthcare providers to implement a complete ecosystem of computing and sensing machines that can communicate themselves to assist the ailing people. The descriptions of these technologies in short are:

ADR: This technology can detect the adverse drug reactions within time, can prevent the lethal dose of any drugs to be a push into a patient's body, make a real-time alarm for the providers so they can mitigate the emergencies.

WDA: These devices are wearable for patients, and can sensing different vital statistics from the patient body to the physician's monitoring device and nursing station. This system can monitor the medical condition of the patient on a 24×7 basis and physicians can monitor the patient in real time for any immediate action if needed (Solanki Nayyar 2019; Anavangot et al. 2018; Sehgal et al. 2020).

SMA: Here, the patient can authenticate the physician to access their medical data through secure connections. This system is important for UID-based medical record system. Here, the communication through secure channels makes sure the confidentiality of the treatment and the privacy of the patient is maintained. This helps doctors to undergo privileged communication with patients.

EMH: Here, the smart cities and smart medical care system can easily mitigate any disaster situations, arrange available transports and medical supplies to the place, can identify and separate different emergency category of the patients, mark them and access them through the shortest route to hospitals and medical facilities, inform blood bank and arrange medications, etc.

EGC can connect several medical types of equipment and life-assisted machines that connected with the patient and send all the data to the cloud-based system from where the medical workers and paramedical workers can access the real-time statistics of the patient's condition and can track the medication, diagnosis, etc. Similarly, ECP contributed to context-aware healthcare applications.

AAL is used to assist especially abled people, old-aged patients, or patients with physical morbidity to live their life peacefully and risk-free manner. This can sense the patient or especially abled persons position in smart home through several interconnected devices, can assist them to communicate or transport from one room to another room, can detect the position of the patient, prevent them from fall or any other home accidents, alarm them, even call the police or healthcare agencies in emergencies (Padikkapparambil et al. 2020).

m-IoT is enabled patients with co-morbidity to manage their life more efficiently. This is a wearable remote sensing device that can be tracked through smartphone by doctors or patient him/herself. All the vital statistics in real time can monitor the patient's condition, as well as an administered dose of medication, or alarm for any medication required immediately (Singh et al. 2020; Dhull and Singh 2020). For example, a diabetic patient can monitor his/her blood pressure, blood glucose level and can have an alarm of requirements of insulin shots or any hypoglycemic condition.

Apart from these, information, communication, and technology-based healthcare communication system (ICT) required IoT-based technology to maintain health education in different parts of the country, especially in health education for the population in a remote area where the resources are constraints.

2.2 Healthcare Applications of Cloud Computing

Cloud-based computing in the healthcare delivery system has an impact on using different technology-based healthcare systems. The most prominent areas are telemedicine where the patient and doctors are connected through teleconferencing methods and IoT-based system can monitor all the biomedical signals of the patient in real time which can be stored in cloud-based system and physician can observe all the data from the cloud-based secure system at any time. Moreover, medical records can be based on this cloud computing where physical storage has no use. A physician can access it through a secure line and huge healthcare data can be stored. Through this cloud-based system, all the real-time medication and other vital statistics of the patient can be accessed by an app or Web server-based cloud (Fong and Chung 2013).

This cloud computing can be the interface with UID for the patient medical records which can be updated by various IoT devices and can be accessed through Web servers. Every hospital has one unique information system and through the link provided by the government or other means, the hospital and health ministry can separately access the data of the patient. Based on this, the treatment and different medications can be compared and the best path of treatment can be discovered. Government agencies and insurance companies can use this database to maintain transparency. This facility can be tracked by the patient relatives who need information and who bear the cost of the treatment. Cost-effective analysis can be done through this even clinical audit too. This is predicted that cloud-based businesses can cover 80% of the total businesses by 2020 and the COVID situation increases the chance (Ahuja et al. 2012). The cloud-based healthcare management applications like electronic medical records (EMR) can store all the patient-related data and cloud-based analysis of these data facilitate better patient treatment. All the data that are stored can be analyzed with the use of a machine learning program. This facility gives a chance to store and analyze all the patient diagnosis data and can indicate several points based on experience which usually in physical form can be hidden from a physician (Cloud Computing in Health Care 2020). The hospital or clinical information system containing online appointments, billing, registration, medical record, diagnostic reports, accounts, audits, insurance claims, and more services can use cloud-based systems. Like NetApp hybrid cloud-based services (Netapp 2020) and Nintex which promote safe patient care services through cloud-based models and secure connections (Nintex 2020), or using several online cloud-based systems to store, secure, analyze, retrieval system promotes better patient care as well as cost effectiveness of the delivery system.

In India, Media Lab Asia under the Digital India Corporation with the help of different Universities and institutions like NIT Durgapur, Jadavpur, and Calcutta University, sets up different health kiosks in Birbhum and Sundarbans area where the patient comes and get in touch with e-health sensor kit. This is a cloud-based infrastructure where the sensor-cloud interface is present and all the health-related data of patient through e-health kit are sent to cloud and doctors sitting in a different area as Kolkata may directly access the data and communicate with the patient through video conference, even prescribed medicine that can be downloaded and printed in the kiosk. This is an example of telemedicine implementation which can be accessed by Android-based apps or using a smartphone (Media Lab Asia 2020).

2.3 Future Healthcare Applications of IoT and Cloud-Based Services

Nanotechnology (Nayyar et al. 2017), artificial intelligence, and the advancement of computing technology increase the chance of new inventions in healthcare fields. Robotic surgery is already initiated in different parts of the world (Batth et al. 2018). The minimally invasive surgery was started in 1987 and getting popularity among surgeons and patients' day by day because it was cost effective and rehabilitation is faster than normal surgery. The recovery rate is also higher and loss of blood and other health-related problems are minima Singh et al. (2020). Using PUMA 560 (Davies 2000) and recently the ARTEMIS system (Schurr et al. 2000) are examples of robotic surgery. With much more precision and using mobile devices to perform the task, using IoT and cloud-based technology, one surgeon now can perform surgery using a robot from a remote position. It can reduce the error, experts can do it from remote positions, save human life as better support, and reduce the chance of cross-infection and nosocomial infection. Now the use of IoT and cloud computing gives the connections to control the robots, now the robotic limbs also use in prosthetics for rehabilitation for a patient with limb loss. It can help specially abled persons to lead a normal life.

Other future applications are based on wireless micromechanical sensors (MEMS) which are tiny and the collection of these is called smart dust (McQuee (2018). These sensors can be taken orally by capsule or can be injected. The main work of these smart dust is getting inside the body of the patient and monitoring the health-related data in real time which can be monitored through a smartphone or Web-based interface. By nanobots, the smart dust can be used as diagnostic techniques and even used for micro-surgery. It can be used in a medical emergency. To detect the actual condition of the body from internal smart dust can be used. It can make a 3D copy of the internal organs and reduce the use of a scanning system which may have radiation hazards. Thus, robotics can serve the healthcare system collaborated with modern AI, machine learning-based models, and IoT (Lanfranco et al. 2004).

Apart from the cloud and IoT-based monitoring system, other uses of IoT and cloud computing system are digital tracking system of drugs. When drugs are administrated and other related data may be considered from this FDA-complied medicine tracker system (Proteus Digital Health 2017). Here, it can indicate the medication-related data easily to physicians and nursing stations and can alarm the patient him/herself.

Using all of these systems, the smart hospital concept can be developed. A smart hospital can use biosensors, embedded technology, RFID, cloud storage, wireless communications to make an ecosystem of integrated hospital information system which can be accessed through a Web-based or smart phone and can control or monitor each aspect. Here the online booking to tagging of the patient, tracking the patient through the ward, tagging all the medical data and diagnosis system of the patient in a single cloud so every information can be stored, monitored, and analyzed through machine learning and AI. One limitation is IP-based problems where all the mechanism may have different IP addresses and can cause integration problems. But due to big data and IoT combinations, we can take care of the problem. Here, error-free treatment and cost-effective medications can be done. Even the maintenance of low power consuming smart electricity and automation can increase the hospital's efficiency. Sterile supply with proper tagging which can indicate the expiry date and can be taken to the department without using it. Same as the linen and bedding of a hospital can be tracked from bed to laundry to linen supply. So, IoT is not only effective for medication and treatment but also general management and sufficiency. The green hospital concept can be implemented through this IoT and cloud-based systems. Biomedical waste management is one of the vital areas today. Tagging and tracking system easily identifies the clean and dirty pathway and secure cross infections from biomedical wastes. This system can track the waste generated and treatment to audit and mitigate cross-infection from the source (Dubey et al. 2020).

The future healthcare system not only eases the mitigation, diagnosis, treatment, morbidity reduction, and decreasing mortality rate, but also becomes cost-effective and provides quality treatment. But this world with technological advancement becoming more and more volatile, uncertainty, complexity, and ambiguity (VUCA) filled with each sector. Every year the modern technology becomes obsolete and new technology comes up. Rapid changes in technology make this world more volatile and walk toward uncertainty. Even to connect all the IoT-based devices makes it more complex and to use the right technology sustainably makes ambiguity. For current leadership, to understand this VUCA world and respond according to this is most important (Vuca-World 2020). In health care, the use of technology changes every day, and cost and training associated with that machinery are costly. Quality costs at first but it saves the actual cost in long run. But ever-changing technologies disturbed the sustainability of the platform basis on which the healthcare delivery system operated. This VUCA model helps the search for sustainable technology and applies that to reduce the stresses.

The hacking and other technical glitches can destroy technological advancement. Security and connectivity issues are there. Any Internet connectivity problem can destroy the whole patient care management system. Low power backup can send the whole scenario in the primitive era. Hacking can fatally change the patient care system. So, lots of challenges can be faced in near future with technological advancement. These challenges should be resolved efficient manner to cooperate with the technology to make it in favor of a sustainable ecosystem.

3 Issues Behind the Use of Electronic Medical Record Based on IoT, and Cloud Computing and UID Interface

The Indian healthcare delivery system consists of both public and private healthcare entities. Health care is in the concurrent list of the Indian Constitution; thus, it is the joint responsibility of state and national level ministry. Indian healthcare delivery system in government is based on four levels as National level, State level, District level, and Panchayati Raj level (Park 2015). India needs a strong healthcare system to deliver for 1.3 billion population. India is likely to become the third largest healthcare market by 2020, providing around 40 million jobs, during 2016–2020 India expected to grow at a record CAGR of 17.69% (Indian Brand Equity Foundation 2020). India has a total of 529 medical colleges in 2019 FY, total registered medical practitioners by IMC are 1,154,686 as of 2018 and the nurse–patient ratio is 1:483 (Indian Brand Equity Foundation 2020). 3 million beds are required to achieve 3 beds per 1000 population within 2025 (Indian Brand Equity Foundation 2020). All of these data are showing the importance of the healthcare delivery system in India. Government opens many cloud-based interfaces for the patient to healthcare providers. India also has huge private healthcare providers in secondary and tertiary health care where diagnosis and specialty care are given. All hospitals need to handle a huge patient database. The everyday large numbers of inpatient and outpatient records are created and need to be stored as per law. The medical record is an important document which is property of the hospital or nursing homes but at the same time a confidential document which can only be produced in front of judiciary or can only be released when patient give their consent to do so.

It is better to store electronic medical records as a physical medical record needs a much bigger area to store, and more costly to maintain and retrieve when required. It is easier when the medical records are maintained electronically as it is easier to store for unlimited time and can send to different third parties as notifiable disease notice to the government, the court summons, or insurance companies. When the patient again comes to the hospital, the hospital can easily retrieve the electronic medical record data using the patient identification number. Medical records are also a headache for the patients to maintain it chronologically and produce it every time required.

When patients go to another provider or any health-related emergency happens on the road or another part of the country, often they do not have the medical record with them. They may produce recent health-related documents but the medical history of past years maybe not present with them. Also, different hospitals do not rely on other hospital's reports. This problem persists and treatment delays for repetitive diagnosis. So, to reduce the physical medical records it is easy to share electronic medical records more easily with the respective healthcare providers.

The next question is how to share different hospital data with one single platform? If all the data are shared in one single platform then it is easier for all the healthcare providers in the country to access the patient medical records without any delay. The patient only needs to carry the identity proof and only to share the consent to the respective hospital to have an access to the patient's data. Through these processes, the health for all slogan can be achieved within a timeframe. That is the main objective of this study. To achieve this, IoT-based services and cloud-based healthcare facilities need to implement all over India basis.

Why online patient care database needed for the country? It has several advantages. As India is suffering from the COVID-19 pandemic right now along with the whole world, the patient care database is essential to initiate the right care for all. Thus, it can have big data to analyze the characteristics of the pandemic in a different part of the country, the treatment procedures and can start a hypothesis for the best possible care. It can deliver a comparison of different medical care to choose the best one. The single cloud-based electronic medical record can provide the best and shortest clinical procedures to fight against one disease. Medical records are not only monitored by the healthcare experts but can send reminders for any current medications or track immunizations. This record reduces the manual work for herd-immunity and automatically indicated the immunization cover. It can prevent misuse of prescriptions and drugs by a patient or reduce the self-medication practices in India. Government insurance and other insurance companies can track and deliver health insurance claims more easily and speedily manner. It can track any epidemic and endemic situation anywhere in the country and send an alarm to the policymakers. Through it, mitigation for any accident or injury due to natural disasters can be managed. This will create clarity and transparency of treatment and costs.

Now why IoT and cloud-based healthcare facilities need to establish electronic medical records? Without a cloud interface, all healthcare providers and health and family welfare ministry cannot access the database. And IoT helps the hospital to track and monitor a patient's condition which must require access to the medical records. The real-time monitoring systems may update the medical record from time to time. Doctors may have accessed the real-time data over the electronic medical record. Like if sensors are attached to a patient's body for blood glucose maintenance, and the machine updates the medical record from time to time, then no need to go to doctors or diagnosis. Doctors can easily access the blood glucose level of a diabetic patient and average the level. If any asymmetry is detected then a doctor's appointment may book automatically or alarm the patient to do so or to have emergency medications.

Unique identification number are those based on which population of a country can access the different government and other facilities and use the number as an identity card. Here in India, the Aadhaar card and Aadhaar number is working as unique identification number or UID. Through this, different government facilities can be accessed. Different identification cards like ration card, voter identification, PAN number, bank accounts, SIM card number, LPG gas subsidy, etc., are linked with Aadhaar card mandatorily or voluntarily. Currently Indian started the e-health portal and some facilities are accessed through Aadhaar card as a patient identity. 1.21 billion Aadhaar card connections are there in India and almost full populations are covered under it. Already the base for Aadhaar card with biometric data is there and already it is connected to the various government portal. Thus, to use it, save the timing for the people and government to enroll all for a patient identification number. Using the national health portal and other government services and link the Aadhaar card to make it an identity card for the electronic patient care management system of India is an easier solution. Various national programmes like Pradhan Mantri Jan Arogya Yojna (PMJAY) can be linked with the Aadhaar card to facilitate the world's largest health insurance program (National Health Policy 2020). The future of the Indian healthcare system needs reform and this can be the start to modernize the Indian healthcare delivery system. One just needs to link an Aadhaar card with the government portal and can avail of all the facilities. Hospitals need to access the Aadhaar number to access the patient medical record with real-time updates. The program may be complex but once initiated, it can be helpful for the patient and doctors. As Aadhaar stored the biometric data, deceased unidentified patient or accidental cases may be accessed through biometrics. The patient can give their biometrics if they do not have access to the Aadhaar card at that time and the hospital can start the treatment based on biometric identification. In normal cases, the patient has to show the

Aadhaar card and give permission to the hospital to access the specific medical records of the patient. Practically the use of physical medical records will be obsolete and hospitals need not store the record as it is easily stored in the cloud-based database. Analysis of the clinical data will be easier for the Indian Medical Association or ICMR to identify best clinical practices. Using big data and analysis of clinical data can invent or discover new clinical pathways for treatment and trials. Using this system, many patient-related data can be analyzed for national policymakers to introduce cost-effective measurements to target the lacking areas. Through this, the authenticate data can be accessed and analyzed to identify the gap and determine the solution.

4 Basic Model to Use UID and IoT, Cloud-Based Computing System

India already started to collaborate with different educational and technological institutions for implementing an e-health system. The national health portal started the e-health portal which describes it a lot. Its main objective is accessibility, quality, affordability, lowering of disease burden, and efficient monitoring of facilities for the citizens (Mogli 2006). Portal indicates a total of 10 E's benefits in detail. They are efficient, enhancing quality, evidence-based, empowerment of consumers and patients, encouragement, education, enabling, extending, ethics, and equity (Mogli 2006). India is already implementing to connect UID with health and based on these 10 points the discussion is going on to how to implement the database of the electronic medical records. So, first, the discussion will be on electronic medical records and its connection with the UID database cloud.

4.1 Electronic Medical Record

What is a clear medical record? The electronic medical record is under the hospital information system where all the doctor's notes, nurses' notes, diagnosis reports, medication reports, pharmacy indents, other indents like linen, dress, etc., are in a chronological manner. All the departments that are collaborating to treat the patient have been included in the medical record. Physicians are involved to learn the medical record of a patient to strategize the diagnosis and treatment part. With the help of the chronological diagnosis and medication report, the treatment chart is prepared and a logical treatment pathway followed. This record is evidence of treatment. Thus, the maintenance of it is of utmost importance. The electronic medical record is associated with all the departments that are under the hospital information system. Here, the IoT has scope to connect with the hospital information system and medical record. At first, let see the traditional design of electronic medical record.

A traditional electronic medical record consists of several subsections like admission department and inpatient, ward management, medical, surgical, laboratory, radiology, billing, accounting and finance, pharmacy, linen, housekeeping, canteen, nursing information system, general supplies, etc. All the computing machines are interconnected through servers by local area network (LAN) and wide area network (WAN) system. The complete hospital information system is a connection of Webs from many departments broadly administration, registration, diagnosis for inpatient and outpatient, admission, emergency, pharmacy for both inpatients and outpatients, housekeeping, maintenance and heating–ventilation–air condition (HVAC), telecommunication and prebooking, finance, human resources, TPA, corporate section, public relations, marketing, operations, etc. Using several system analysis and design approach and hierarchical input process output (HIPO) charts for several broad and subsystems makes the electronic hospital information system operational.

A traditional medical record system has some forms of modules. These modules need to be designed efficiently. They are the registration module, appointment module, record tracking module, and admission and discharge processing module (Singh et al. 2020). The registration module should contain the patient name, sex, date of birth if available or age, type of patient like paid, corporate or TPA, marital status, full address, contact number, identity card if any, relative's name, relation, and contact number, etc. The registration number is generated automatically after the registration processes. The patient needs to link this unique registration number whenever he/she will arrive at this hospital. The day and time should be recorded with this so the real-time monitoring system can be initiated. After this, the patient should enter for a physician's appointment. Here the registration number of the patient automatically fetched the data of the patient. Department master entry and doctor's entry are there with the list of all holidays and doctor's duty roaster. The appointments are automatically fixed and the patient gets a confirmation via physical copy or message to the contact number. Then the vital parts are coming, record tracking module. Here, all the doctor's note, nurse's note, prescription, pharmacy items, miscellaneous and general items, cloth and linen, diagnosis module included laboratory, radiology, and other facilities are connected through the hospital information system module. Through the registration number of the patient, all the reports and item lists are recorded against the patient's medical record. All the samples collected from the patient to the return of the report can be tracked and accessed by physicians from their LAN, WAN, or cloud-based machines like personal computers or tabs. All the reports can be tracked by this centralized electronic medical record system. Admission and discharge module consist of inpatient registration and admission, ward and bed management, department, operation theater, ICU, discharge details, medico-legal cases, paid/corporate or TPA, etc (Singh et al. 2020). All of the medical records must connect with medical transcript services which may follow ICD-10 standards which is universal.

This is one standard electronic medical record system. Now this medical record system is helpful for clinical audits. It can take different statistical data to control the quality of the treatment like mortality rate, bed occupancy rate, nosocomial or hospital infection rate, the average length of stay (ALS), fatal death rate, caesarean section rate, hospital autopsy rate, bed turnover interval, perinatal mortality rate, post-operative death rate, etc. So medical records not only benefited patient treatment but also for the hospital to maintain quality and standards. These statistical data are measuring units. Thus, from medical record modules, various info-graphs can be drawn to know the current situations.

Electronic medical records save storage time and create access to the patient-related data in the internal database. Using information technology, it will help to retrieve the patient-related data in future time, just to put the registration number or inpatient number of the patient. During the treatment procedures, the time of the treatment can be reduced to use it. Just putting the registration number, patient's history and medication information can be easily accessible. Here, the patient just needs to produce the registration number in front of the front office. Once the patient gets admitted and transferred to the wards, all the medication and diagnoses against the patient are put into the hospital information system and can be accessed against the patient registration number. All the physical documents required tagging systems where the tagging system consists of basic patient identification data like physical files, hand tagging, and others. Thus, the misplace of the samples and files are stopped. All the results from the diagnosis center are directly uploaded to the EMR system so the physician can see that without going to the ward. No need for a physical report and transportation needed to the ward. Through the tagging, no error will appear while testing the samples cause during result generation it should match with the patient's prescription. Due to tagging, the error during surgery is reduced. Basic electronic medical record based on the hospital database management system is the pathfinder for this UID-based medical record maintenance. The basic idea of the electronic medical record is presented in Fig. 1.

Through the database management system, all of the functions from admission to discharge are operational. The physician has an access to the patient database where all the documents are uploaded on a real-time basis.

4.2 Relationship Between IoT and Electronic Medical Record

The Internet of things and the medical record have a very close relationship. As we can see in Fig. 2 when a patient arrived at the hospital and registered him/herself than from that time the tracking is started. There are several procedures to attach the IoT-based technology with the patient and patient belongings. For example, at the time of admission, tagging is attached to the patient's hand, dress, and physical file with a bar code. Even at the time of collecting pathological samples, the tagging with bar codes against the patient is attached. Here, the bar codes are checked before proceedings and reduce the chance of misplacement of the report or any mix of the samples. During surgery, the surgeon must not confuse anything. Here the bar codes can give them the right information before any proceedings. These sensors, tracers, and digital markers reduce the errors in treatment.

The remote sensors can detect the patient's condition from different places like doctor's or nurse's station or they can access it through the app or LAN/WAN-based services. The patient record system updates the real-time patient condition or round-the-clock vital statistics like temperature, blood pressure, glucose level, blood oxygen level, etc. Through this, the treatment decision can be taken by physicians easily and timely. These records can help in case of any medico-legal cases where the treatment procedures are under scanner. The decision making by the expert with the help of authentic machines and within time is crucial to saving the life of the patient. In case of any emergency, the mitigation is simplified.

At the time doctors can access the diagnosis reports remotely and in real time, with no need to wait for print and delivery. This speeds up all the treatment procedures. The authentication of billings can be simplified when the indication of procedures is updating in the medical record. After discharge, all the unused medications need to refund to the pharmacy also in automation mode. Through RFID, the physical files and other documents can trace and loss proof.

4.3 Relationship Between Medical Record and Cloud Computing with UID

Unique identification number is mainly used as Aadhaar card in India. All the identity cards like a voter, PAN, ration, even banking, and other government subsidies can be accessed through Aadhaar card. It also connected the phone number of the person. India starts the e-health portal and a patient can book or avail of government hospital facilities online using the Aadhaar number or the phone number

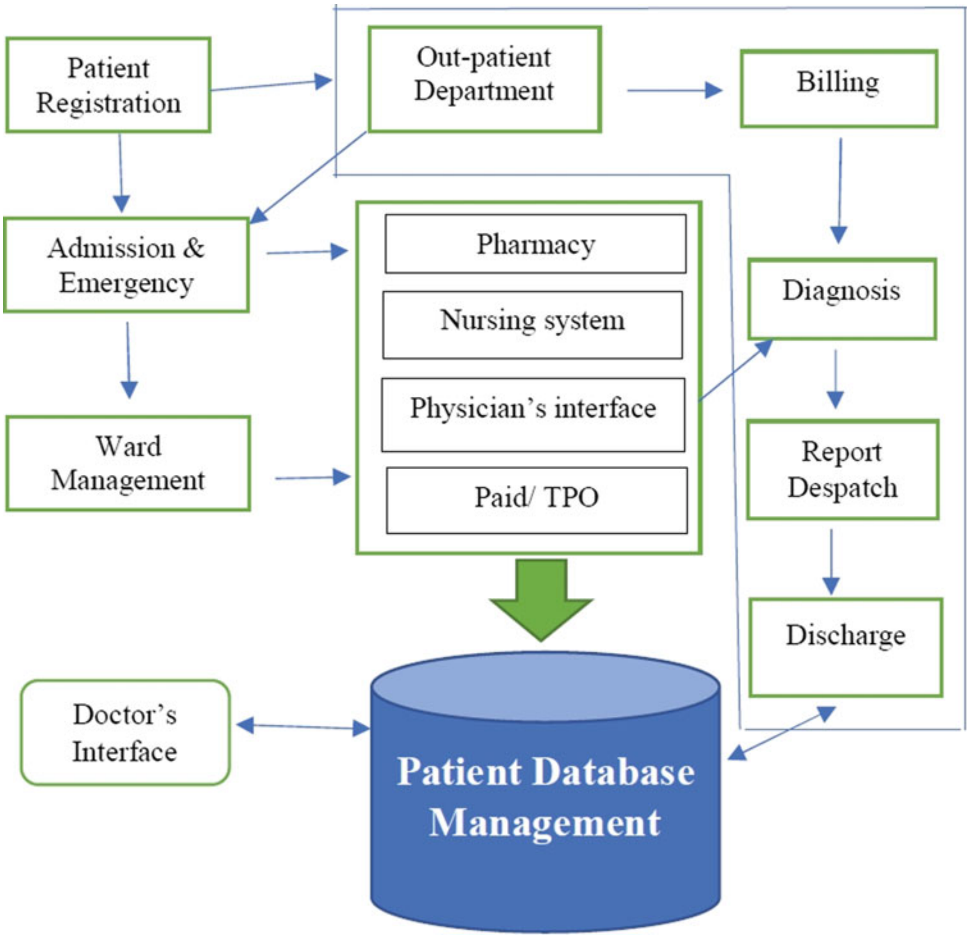


Fig. 1 Simple database management for electronic medical records interface

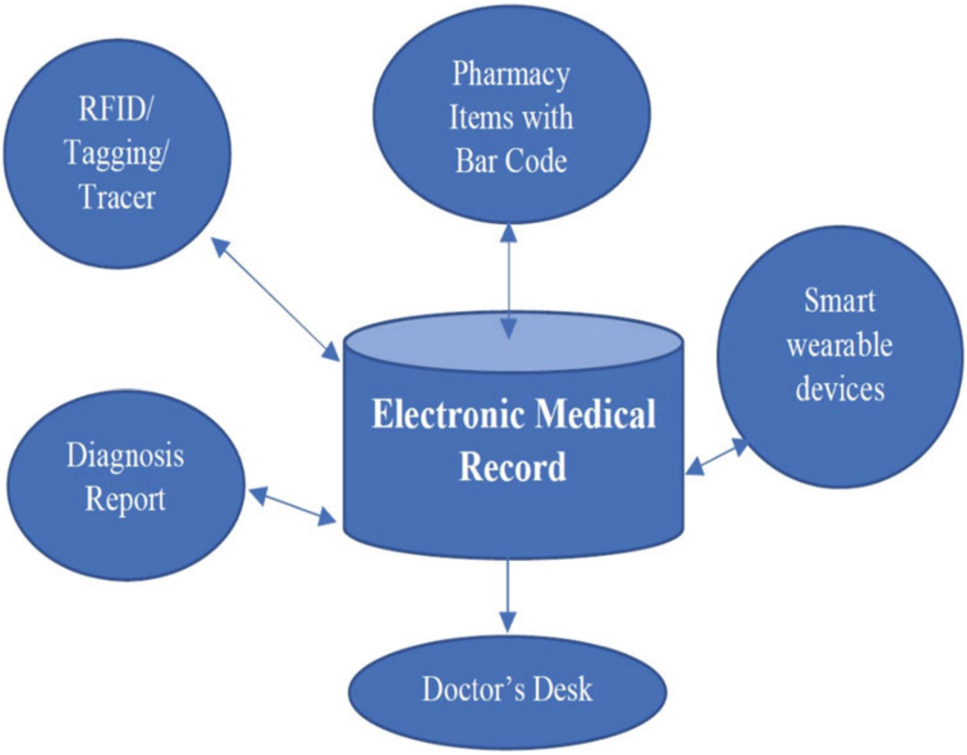


Fig. 2 Block diagram of an IoT and electronic medical record system

linked with an Aadhaar card. The government of India already started digital initiatives in different sectors including health and family ministry. Thus, the UID is already ready to move and an easy option to implement it with the national medical records system.

The UID has access to 1.23 billion population out of 1.3 billion population of India. This UID also stores biometric data of an individual. Through a cloud-based system, UID can be used as a patient identification number through which the medical record of the patient can be accessed. This medical record system can be accessed through one single portal all over India. Smart healthcare systems can be implemented to use this approach. All the health-related tracking and monitoring becomes easier through this. Let us discuss the process of UID and cloud-based healthcare system and online medical record.

Figure 3 shows the proposed outline of the cloud-based medical record database which can be accessed via secure connections using the UID number of the patient. All hospitals, private and public both, have their medical record system module. This module should connect to the unified cloud system. Thus, all the patient database can be accessed through the national patient care information system or database. The patient can give authentication to access the medical record data or a part of the data while other data are stored securely. It will also maintain the privacy of the data. Even the IoT-based sensors or other machinery can update the system in real time. Physicians can access the patient's condition in real time and the patient can access treatment anywhere in the country in any case of emergency. Patients do not need to carry prescriptions because through Aadhaar card access they can produce the latest prescription by a doctor to any healthcare provider or pharmacy. Many other advantages are associated with it. The discussion on different access and advantages are discussed in the next point.

5 Advantages of IoT and Cloud-Based Medical Record System

The medical record system with powerful connectivity that can be accessed anywhere in the country through authentication from the UID holder. This is the first step for cloud-based medical record. When the patient comes to any hospital in India, he or she needs to produce only one identity card, which is an Aadhaar card or just the phone number linked to it. After the authentication, the hospital can access the required healthcare database of that particular patient they need to treat. Here the advantages lay with the access of the healthcare data. The patient need not carry any bulky reports or previous prescription as everything can be assessed electronically. For the prebooking facility, the patient need not carry anything but an Aadhaar card or the phone number to book him/herself for an appointment for doctors or any department.

The hospital need not store any physical form of medical records as it is already in the portal and they can access all the record of their healthcare institutions and can access other records with the permission of the patient. Here the system stores separate hospital's records separately and after full access, one hospital can fetch the record chronologically. This system not only prevents privacy matters but with the past medication history, the healthcare provider can know about the allergy history, co-morbidity, or regular medicines that the patient takes every day.

Through this system, the IoT mechanism that may attach with the patient's body as wearable sensors, real-time update the medical record sections too. Through this, one can observe regular heart rate, blood pressure, the glucose level in the blood, COPD mitigations, and maintenances from anywhere. But as the IoT updating the medical record charts every day, with the authenticate from the patient, the treating physician may get real-time data without the repetitive pathological or radiological diagnosis. The patient also gets a notification for any medication regular interval in his/her phone or pager. Even patients can receive an alarm in case of a repeat visit to a physician or any routine diagnostic tests.

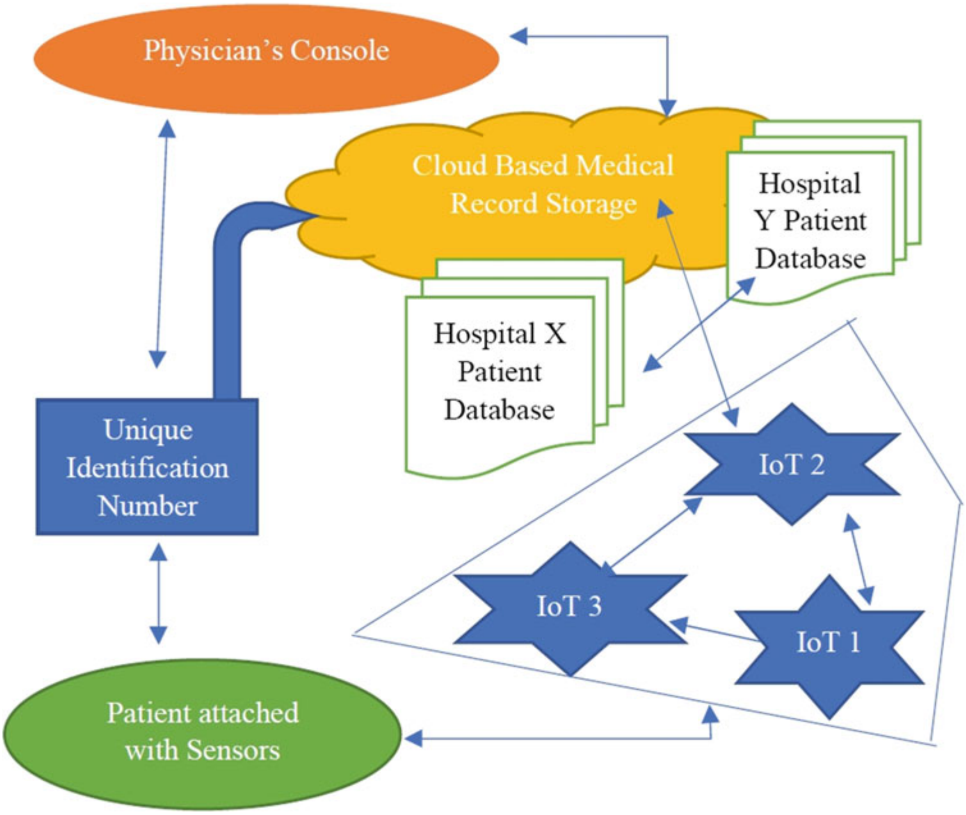
The patient can use the card or phone number confirmation in any pharmacy to buy medicines without a prescription. But he or she cannot buy extra medicine as the pharmacy but can be linked with the database. If any patient buys over medication or any medicine without the prescription, this system easily identified it and prevents the patient from a drug overdose.

As the patient has a special identity card, during an emergency the patient can get booking an ambulance from nearby hospitals using some app-based or Web-based services. In case of an accident, the biometrics from the victims can identify them easily and, in this case, the healthcare provider can access the database with special permission. Here, the speedy mitigation of any disaster situation can be handled skilfully.

With a single database, the government can easily be notified of any notifiable diseases. Healthcare providers can take precautions for any communicable diseases. The patient facilitates treatment not only for current diseases but also for co-morbidity too. The future course of action will become easy when all the health factors are known to the facilitator.

One patient can receive the best possible treatment as the database can be used for research purposes and with this huge database one can learn the fastest and safest route of treatment to analyze the data. The data is available without disclosing the identity of the patients and the best course of action can be suggested through this. Big data analysis, machine learning, and artificial intelligence are required to analyze the huge data and discover a different pattern of the

Fig. 3 Cloud-based medical records, IoT and sensors monitoring patients and UID



same diseases, compare treatment, and calculate the average length of stay and incidence–prevalence ratio. Thus, the government agencies can easily compare the different courses of treatments for a similar disease and indicating the future course of action.

Through this facility, the government agencies can also monitor the hospitals simultaneously about their response toward patients. The clinical trial will become much easier to test it on a large population at one time. In any medico-legal case, the evidence may have stronger power as it may show the real-time performance of the treatment and real-time data.

Government agencies can mitigate any epidemic or endemic situation to get alarmed about the patients from these online medical record facilities. It can observe the recent areawise incidence and prevalence to identify any epidemic or endemic situation promptly. Even the intelligence system can indicate the current situation and give an alarm to the respective agencies to mitigate the situation. Even it can indicate and monitoring the pattern and give alarm in case of any specific diseases.

The hospital's response time reduces the healthcare costs for both the hospital and patients. Online access to the patient information system reduces physical medical record maintenance and handling costs. The intelligent IoT with medical records gives a warning about the patient's health conditions thus the response time gets reduced. The medication history of the patient warned the inpatient pharmacy and they can easily indent regular medicines the patient taking other than the current problem. Like medication of diabetes if the patient has it but that is not the actual present problem for which he/she comes to the hospital. Recently COVID-19 situation allows us to know how co-morbidity exists and how to control it. With this smart analysis system, through ICD-10 coding compilations, all the diseases registered in this portal are officially reported to the government automatically on notifiable diseases, and actual data transparency is maintained in that case. Live prevalence and incident rates can be monitored through online surveillance.

This surveillance is helpful for the government authority to calculate different statistical data and mitigate the situation beforehand. It can mitigate the epidemic or endemic situations more easily and respond rapidly. The detection of it will be easier because of the real-time patient information data are uploading to the database.

In COVID-19 or similar situations, it is helpful, because the medication and treatment procedures are updated on a real-time basis. All the treatment procedures and diagnostic procedures will be updated in real time and research organizations can analyze the data in real time to discover or innovate the most appropriate treatment methods.

Through this system, the general risks associated with some treatment or procedures are easily detectable. The adverse effect of drugs can be identified through this system. A patient with a particular disease or co-morbidity may react differently with some drugs. In today's world, many drugs are usually used in third world pharmaceutical market which may be removed by FDA or similar organizations from the first world (Singh et al. 2020). This is obvious that some drugs may hurt different co-morbidity or different age group. Through this real-time database, it is easier to identify such effects through details analysis of the huge database at a single time. The propositions and hypothesis tests may have enough data to prove that. Different surgery procedures and success rates with associate risks can be identified through the database by researchers. These will improve the success rate of the treatment and reduces the associated risks.

When we can mitigate the risk, we can also increase the quality of health care. Through different accreditation agencies like National Accreditation Board for Hospitals and Healthcare Providers (NABH) (National Accreditation Board for Hospitals and Healthcare Providers 2020), Joint Commission International (JCI) (Joint Commission International 2020), etc., one hospital tried to acquire quality accreditations. All the accreditation agencies are focusing on strong monitoring and controlling technology to protect the life of the patients and cut the excess costs associated with it. In long run, the quality cost is also reduced as it reduces the error and wastages. A clinical audit may take help from the data stored inpatient information system.

In NABH, there is main two parts of the standard of the hospital, patient-centered standards and organization-centered standards. Both standards are divided into five substandards each. Here is an organizational-centered standard; the last point belongs to the information management system (IMS) (National Accreditation Board for Hospitals and Healthcare Providers 2020). Here the NABH focus on standardizing the formats for data collection and manage necessary resources for the same. The documentation should be timely and tagged with the date. With the help of an online database, all the necessary clinical information will be updated timely and chronologically to facilitate timely decision making. All the accreditation boards or councils prescribed standard medical records. Under IMS standards, NABH prescribed a complete medical record with a unique identifier. Every hospital has its medical records followed by its formats of it. A national standard format that complies with most accreditations authorities is required to design the medical record formats.

The medical record should comply with patient identification data, date, time, and signed and all the documents uploaded timely and chronologically. The author of the entry should identify accurately. The medical record should available 24 h any time and electronic medical records have access through this for 24 × 7. Medical record reflects the continuity of care (National Accreditation Board for Hospitals and Healthcare Providers 2020).

India's medical insurance is mostly covered by the out-of-the-pocket model. In 2018, FY India covered around 35% of the population with health insurance coverage where maximum coverage is by government-sponsored schemes including Rashtriya Swasthya Bima Yojna (RSBY). A total of 357.1 million population is covered under a government-sponsored health scheme, 72.9 million under group business (excluding state-owned), and 42.1 million individual insurance (Keelery 2020). In July 2019, around 125.7 million families are joined with Pradhan Mantri Jan Arogya Yojna (PMJAY) (Indian Brand Equity Foundation 2020). So, the database is huge and the scope is there. If the healthcare database and all the insurance program can be joined with the portal then the patient need not produce any insurance document while admitting to a hospital. The insurance companies get automatic notification of the admission of the patient. The documents are provided by the hospital to the insurance corporation through a secure portal. During the discharge procedures, the insurance corporations get an automatic alarm and can access the patient information system database to provide the final bill covered by the company. Thus, the time taking TPA procedures after discharge was reduced, and the process was recorded properly for the proof of the claim. Different government group policies like the ESI facility also can be connected to a claim. Here the manual documentation not required and real-time insurance claim can be settled without any communication gap between the health provider and insurance corporation.

Now, the advantage of IoT linkage on the patient information data is somewhat more radical. A cloud-based patient information system does not only serve the patient to join a universal platform of community health care for India, but a futuristic healthcare delivery system may take its base. All the IoT devices to maintain a smart hospital has an impact on the patient treatment program. Like barcoding and tagging a patient, it prevents any accident and misplacement. It reduces different medication errors and miscommunications. Now how it can help in every department and how the IoT-based smart hospital maintains the utmost care to the patient are described below.

The IoT-based patient care devices transferred real-time patient information to the nursing desk and doctor's desk. From the desk, physicians and nurses can monitor the real-time patient health data and mitigate any condition immediately. The patient relatives can access the patient-related real-time information that they want to know.

In India, the confidentiality of the patient's information is a big challenge. Patient relatives are anxious about the cost of the treatment and care given by the hospitals. Many cases are there in India where the hospital or doctors are blaming the over-cost of treatment and quality of treatment. The IoT cloud-based patient information system for the patient relatives to a limited number of options is to track the cost and all the treatment facilities given by the hospital in real time. This may decrease the anxiety of the patient relatives. One transparency of the treatment and cost matters added value to the hospital.

The government authorities can access the real-time patient information data and cost associated with it easily. It resolves many issues like healthcare costs and malpractices. E-governance for the healthcare field can be implemented through these clouds-based and IoT-based patient information system services.

The nosocomial infection and its prevention can be monitored through the patient information system by government agencies or third-party agencies to minimize the chance. The live statistical data on hospital infection rate or post-operative infection rate is helpful to analyze the actual root cause of the hospital infection.

Another help of the IoT and different hospital's portal's access in a single window is required to facilitate the patient information system. Through this, all the hospital-related statistics like a vacant bed, occupancy rate, vacant ICU beds, ventilators, life-supporting devices, ambulances, blood bank statistics, and availability of different blood groups may be synchronized and accessed through an app or Web-based e-health portal. Through this, the patient can choose the hospital without any chance of not getting an appointment and beds. In any disaster situation, the mitigation and transport of the patient to the nearest hospital are easier through this information. For emergency requirements of the blood or life-supporting devices' availability, this single portal with real-time data and prebooking or preorder system facilitates patients a better opportunity to get the chance of treatment more efficiently.

During the COVID-19 situation, state governments started these types of apps and Web-based services separately with collaboration with different government and the third party. But for better care and policy, the single portal system is helpful for more patients (Fig. 4).

Tracking of the immunization programs and vaccination programs, the tracking of the different government disease eradication programmes will be more efficient and accurate if all are connected through the e-health portal. Like when the mother and child health programs are running, based on the mother's Aadhaar card all immunizations and other vaccinations are updated through the portal in real time. By this, the policymakers can easily identify and bridge the gap between actual and targeted services.

6 Limitations of the System and Idea to the Response that

Like every system, this system also contains some limitations. The limitations are associated with many conditional reasons and facts. Nearly less than half of the population has access to the Internet and smart phone (Bureau 2019). For the prebooking facility and to search for nearest hospitals with a vacant bed or nearby blood bank with the availability of the required group, nearly half of the population has no opportunity to see the live statistics and book. Here the old technology like SMS or over phone communications with customer care helpline has importance. Additional cost is required to run this system side by side with full fledge online digital India initiative.

The next level problem is associated with the digital e-health initiative and online patient information system's connectivity. 4G technology is there for the long run basis and high-speed connectivity is there. But during the lockdown period, people tried to go online more time and due to work from a home initiative by different corporates, the users spend more time online. This congested traffic over communication hits the Internet speed and download speed in India (Majumdar 2020). If India needs to go digitalized in every service, Internet connectivity through 4G or 5G technology is not enough. The connectivity issues should resolve before we take digital initiatives for all citizens.

As UID is used everywhere in India, the next question comes with the e-health initiative and the patient information system is 'Security' of the data. It is obvious that through many spurious apps the data breach is easy. Recently different articles show the security breach over social media and even UID (Bureau 2018; Silverstein 2019). This volatility and security of data need to be resolved in a very secure manner. This online is new normal and needs more work on upcoming issues related to it.

Different IoT-based mechanism may have different adaptability and IP addresses. Thus, the communication between different IoT mechanism is hard. End-to-end encryption data transfer models with different platforms may not be possible at a time. So, we need to work on this facility where different technologies are used to make connectivity with different devices and initiate all the communications in a single platform like a cloud-based patient information system is not an easy matter.

For a country like India, where computer literacy increasing day by day and more users adopted different online or digital platforms, an information. communication, and technology (ICT)-based educational system needs to

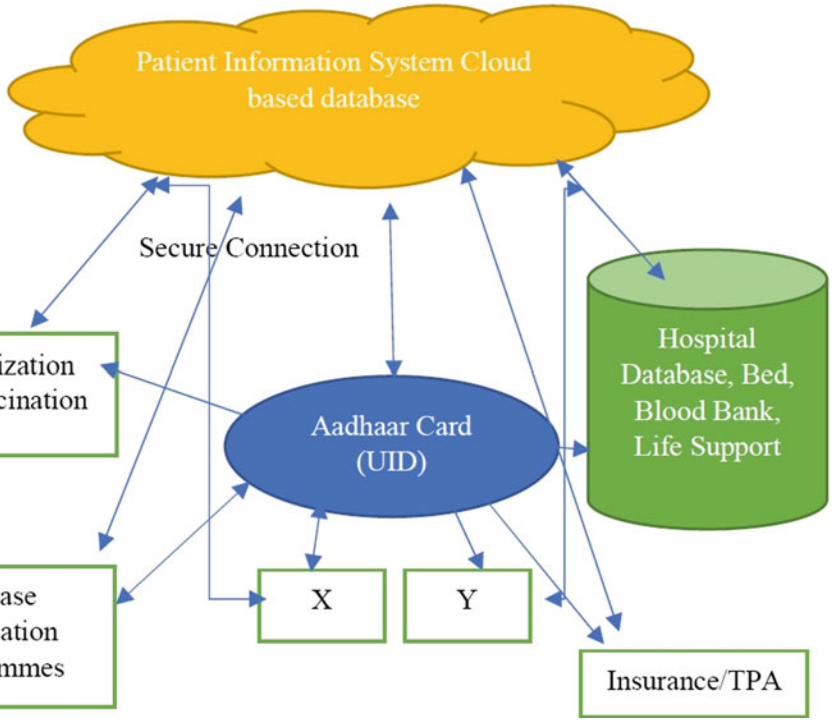


Fig. 4 Relationships of a different database of government and facilities in a single-window e-health system and unique patient identification number

implement in all over India. This will help the population to interact with the new VUCA world (Vuca-World 2020).

To address the security problems, an introduction to blockchain technology has the answers. As through blockchain, the major advantages are: it will secure access to the consumers, it only shows the data required to or important only for the purpose to the healthcare providers and other data cannot access without the permission of the patient (Singh et al. 2020). If anyone wants to change some data, it is not easy to change it without proper permission. Blockchain can be used in IoT-based service accesses, remote controlling of the medical devices, database analysis, encrypting the data related to confidentiality issues, etc (Mettler 2016). It can only fetch the information from the information packets and get back to the healthcare providers. Thus, it reduces the chance of data leakages.

7 Conclusion

With the digital India initiative, the idea behind introduces a patient information database with a single window, and UID-based access are comes out but this is not a new idea. With the growing digital initiative all over the world, this is a replacement for the manual single-window system. Many countries initiated a different kind of healthcare delivery models. Some model goes through single-window government initiatives like UK, Spain and some European countries have national health insurance model like in Canada, or mixed model in India like blend of government, private and out-of-the-pocket model (Chung 2017). This digital initiative can bridge the gap between the patient and the healthcare providers and maintain the quality and accessibility in low cost or minimum cost model.

IoT and cloud-based technology are disrupted technology mostly and can join to database analysis through machine learning and artificial intelligence. Robotic and automation are already there in vogue and IoT can give it efficiency. As the maintenance cost for the cloud computing system is very low compared with the manual system, the cost associated with costly healthcare machines or robotics in long run may reduce.

To digitalize and transforme into a nationwide database of the patient information system, radical changes in the healthcare delivery system will be initiated. The digital transformation helps this idea to maintain health care for all moto efficiently. We should learn about the limitations that may come with the system and the advantages that will happen. Many scopes for analysis and designing of new treatment procedures, surgery, pharmaceutical innovations are there. Let us hope for a better world with affordable, efficient, and accessible health care for all in the post-COVID era.

References

AarogyaSetu App, mygov.in. Retrieved 6 July 2020 from https://www.mygov.in/aarogya-setu-app/.

Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. Retrieved 2 July 2020, from http://dx.doi.org/10.5539/nct.v1n2p12.

Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., & Marrocco, G. (2014). RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of Things Journal*, *1*(2), 144–152.

Anavangot, V., Menon, V. G., & Nayyar, A. (2018, November). Distributed big data analytics in the Internet of signals. In *2018 International Conference on System Modeling and Advancement in Research Trends (SMART)* (pp. 73–77). IEEE.

Batth, R. S., Nayyar, A., & Nagpal, A. (2018, August). Internet of robotic things: Driving intelligent robotics of future-concept, architecture, applications and technologies. In *2018 4th International Conference on Computing Sciences (ICCS)* (pp. 151–160). IEEE.

Bureau. (2018, October 20). 1 bn records compromised in Aadhaar breach since January: Gemalto. Business Line. Retrieved July 11, 2020, from https://www.thehindubusinessline.com/news/1-bn-records-compromised-in-aadhaar-breach-since-January-gemalto/article25224758.ece.

Bureau, P. (2019, January 06). Govt will soon make Aadhaar-driving license linking mandatory: Ravi Shankar Prasad. Indian Express. Retrieved July 5, 2020, from https://indianexpress.com/article/india/aadhaar-driving-licence-linking-ravi-shankar-prasad-5525713/.

Chung, M. (2017, December 2). Health Care Reform: Learning From Other Major Health Care Systems. Princeton Public Health Review. Retrieved July 12, 2020, from https://pphr.princeton.edu/2017/12/02/unhealthy-health-care-a-cursory-overview-of-major-health-care-systems/.

Cloud Computing in Health Care, builtin.com. Retrieved 26 June 2020 from https://builtin.com/cloud-computing/cloud-computing-in-healthcare.

Cole, T. (11th February 2018). Interview with Kevin Ashton-Inventor of IoT. Smart-industry.net. Retrieved June 10, 2020, from https://www.smart-industry.net/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users/.

Davies, B. (2000). A review of robotics in surgery. *Proceedings of the Institution of Mechanical Engineers, Part H, 214*, 129–140. [PubMed] [Google Scholar].

Dell Technology. delltechnologies.com. Retrieved July 5, 2020, https://www.delltechnologies.com/en-in/cloud/dell-technologies-cloud/benefits.htm.

Dhull, S. K., & Singh, K. K. (2020). A review on automatic epilepsy detection from EEG signals. In *Advances in Communication and Computational Technology* (pp. 1441–1454). Springer.

Digilocker services. Retrieved 15 June 2020 from https://digilocker.gov.in/.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Digital India. Retrieved 4th July 2020 from https://digitalindia.gov.in/.

E-hospital cloud. Retrieved 16 June 2020 from https://ehospital.nic.in/ehospitalsso/.

Fong, E.-M., & Chung, W.-Y. (2013). Mobile cloud-computing-based healthcare service by noncontact ECG monitoring. *Sensors*, *13*(12), 16451–16473. MDPI AG. Retrieved 26 June 2020 from http://dx.doi.org/10.3390/s131216451.

Gartner. (2014, March 19). Gartner says the Internet of Things will transform the data center, gartner.com. Retrieved 21 June 2020 from http://www.gartner.com/newsroom/id/2684616.

Indian Brand Equity Foundation, ibef.org. Retrieved June 30, 2020, from https://www.ibef.org/download/Healthcare-May-2020.pdf.

Internet of Things. internetofthingsagenda.techtarget.com. Retrieved 29 June 2020 from https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access*. https://doi.org/10.1109/access.2015.2437951.

Joint Commission International. jointcommissioninternational.org. Retrieved 3 July 2020 from https://www.jointcommissioninternational.org/en/.

Jones, S. B., Jones, D. B. (2001). Surgical aspects and future developments in laparoscopy. *Anesthesiology Clinics of North America*, *19*, 107–124. [PubMed] [Google Scholar].

Keelery, P., & 7, J. (2020, July 07). India—people with health insurance 2019. Statista.com. Retrieved July 12, 2020, from https://www.statista.com/statistics/657244/number-of-people-with-health-insurance-india/.

Lanfranco, A. R., Castellanos, A. E., Desai, J. P., & Meyers, W. C. (2004). Robotic surgery. *Annals of Surgery, 239*(1), 14–21. https://doi.org/10.1097/01.sla.0000103020.19595.7d.

Majumdar, R. (2020, April 09). Covid-19 lockdown: Download speed hit as work from home strains networks. Live Mint. Retrieved July 11, 2020, from https://www.livemint.com/news/india/covid-19-lockdown-download-speed-hit-as-work-from-home-strains-networks-11586425330086.html.

McQuee, M. (2018, July 24). The future is at hand. Hospitalhealth.com.au. Retrieved July 10, 2020, from https://www.hospitalhealth.com.au/content/technology/article/the-future-is-at-hand-970690498.

Media Lab Asia, itra.medialabasia.in. Retrieved 27 June 2020 from https://itra.medialabasia.in/.

M. Mettler (2016). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference On E-Health Networking, Applications And Services (Healthcom)*, Munich (pp. 1-3). https://doi.org/10.1109/Healthcom.2016.7749510.

Mogli, G. D. (2006). Computerization of the medical records. In *Medical records: Organization and management* (pp. 12-15). Jaypee Bros.

Mogli, G. D. (2006). Computerization of the Medical Records. In *Medical records: Organization and management* (pp. 213-234). Jaypee Bros.

National Accreditation Board for Hospitals and Healthcare Providers, nabh.co. Retrieved 2 July 2020 from https://www.nabh.co/.

National Accreditation Board for Hospitals and Healthcare Providers, nabh.co. Retrieved 2 July 2020 from https://www.nabh.co/Hospitals.aspx.

National Health Policy, nhp.gov.in. Retrieved 2 July 2020 from May 29, 2017 https://www.nhp.gov.in/e-health-india_mty.

National Rural Health Mission, Mother, and Child Tracker. Retrieved 25 June 2020 from http://nrhm-mcts.nic.in/Home.aspx.

Nayyar, A., Puri, V., & Le, D. N. (2017). Internet of nano things (IoNT): Next evolutionary step in nanotechnology. *Nanoscience and Nanotechnology, 7*(1), 4–8.

Netapp. Retrieved 27 June 2020 from https://www.netapp.com/us/index.aspx.

Nintex. Retrieved 27 June 2020 from https://www.nintex.com/.

Office of the Registrar General and Census Commissioner, India. Retrieved July 3, 2020, from https://censusindia.gov.in/2011-Common/CRS_2017/8%20At%20a%20Glance.pdf.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 217–243). Academic Press.

Park, J. E. (2015). Health planning and management. In *Park's textbook of preventive and social medicine* (23rd ed., pp. 878-881). BanarsidasBhanot.

Proteus Digital Health, 2017, proteus.com. Retrieved 27 June 2020 from https://www.proteus.com/press-releases/otsuka-and-proteus-announce-the-first-us-fda-approval-of-a-digital-medicine-system-abilify-mycite/. Press release 14th November 2017. Accessed on 01-08-2019.

Ranger, S. (2018, December 13). What is cloud computing? Everything you need to know about the cloud explained. ZDNet. Retrieved July 10, 2020, from https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/.

Schurr, M. O., Buess, G. F., Neisius, B., et al. (2000). Robotics and telemanipulation technologies for endoscopic surgery: A review of the ARTEMIS project. Advanced robotic telemanipulator for minimally invasive surgery. *SurgEndosc*, *14*, 375–381. [PubMed] [Google Scholar].

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IoT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Silverstein, J. (2019, April 04). Hundreds of millions of Facebook user records were exposed on Amazon cloud server. CBS News. Retrieved July 11, 2020, from https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/.

Singh, K. K., Siddhartha, M., & Singh, A. (2020a). Diagnosis of coronavirus disease (COVID-19) from chest X-ray images using modified XceptionNet. *Romanian Journal of Information Science and Technology, 23,* S91–105.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020). Internet of Things in pharma industry: possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Academic Press.

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020c). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet, 12*(4), 61.

Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In *Handbook of Research on Big Data and the IoT* (pp. 379–405). IGI Global.

Vikaspedia definition, Vikaspedia.in. Retrieved 20 June 2020 from https://vikaspedia.in/e-governance/digital-india/e-health-portal.

Vuca-World, vuca-world.org. Retrieved 29 June 2020 from https://www.vuca-world.org.

White, C. C., III, & Cheong, T. (2012). In-transit perishable product inspection. *Transportation Research Part E: Logistics and Transportation Review, 48*(1), 310–330.

Internet of Robotic Things: Its Domain, Methodologies, and Applications

Amos Orenyi Bajeh, Hammed Adeleye Mojeed,
Ahmed Oloduowo Ameen, Oluwakemi Christiana Abikoye,
Shakirat Aderonke Salihu, Muyideen Abdulraheem,
Idowu Dauda Oladipo, and Joseph Bamidele Awotunde

Abstract

Robotics involves design, construction, operation, and use of intelligent machines that possess the ability to sense, compute, manipulate, and navigate environments to monitor events and execute an appropriate course of action. Internet of Things (IoT) on the other hand is a fast-developing novel technology consisting of group of uniquely addressable heterogeneous smart objects or tiny devices (things) interconnected via the Internet to share and process data from different sources. IoT is designed with the goal to "connect everything and everyone everywhere to everything and everyone else." The two technologies, IoT and robotics, have evolved into Internet of Robotic Things (IoRT) by the creation of a synergy between the two. IoRT aims at enhancing the current IoT with active sensing and actuation from robotics. This idea opened a novel opportunity for collaboration between IoT and robotics applications and research communities. However, most application domains of IoT and robotics have not fully explored the use of IoRT. This chapter discusses the (potential) applications of IoT-aided robotics in different domains, explaining how robots can extend the capabilities of existing IoT architectures to make them more knowledgeable and smarter; discuss some of the challenges in the full realization and application of IoRT; and lastly proposes an IoRT architecture for smart library management, an area that has not received much attention in the research community.

Keywords

Robotics • Internet of Things • Internet of Robotic Things • Application of IoRT • Actuation

1 Introduction

Internet of Robotic Things (IoRT) is the merging of two technologies, Internet of Things (IoT) and Robotics (Afanasyev, 2019; Simoens, 2016; Grieco et al., 2014; Whitesides, 2018; Batth et al., 2019; Simoens et al., 2018; Ray, 2016; Sethi & Sarangi, 2017; Vermesan et al., 2017). Robots have been extensively used in solving problems and making them smart by building into them artificial intelligence so that they could be autonomous as much as possible. The need to make robots know about the existence of other robots in their environment so that they could collaborate to handle more complex tasks brought about the multi robot system (MRS) which requires machine-to-machine (M2M) interaction. On the other hand, Internet of Things (IoT) is a fast-developing novel technology consisting of group of uniquely addressable heterogeneous smart objects or devices (things) interconnected via the Internet to share and process data from different sources. IoT is designed with the goal to "connect everything and everyone everywhere to everything and everyone else". IoT has been used in various area such as healthcare, military, industrial processes, business as well as smart city.

A. O. Bajeh (✉) · H. A. Mojeed · A. O. Ameen · O. C. Abikoye · S. A. Salihu · M. Abdulraheem · I. D. Oladipo · J. B. Awotunde
Department of Computer Science, University of Ilorin, Ilorin, Nigeria
e-mail: bajehamos@unilorin.edu.ng

H. A. Mojeed
e-mail: mojeed.ha@unilorin.edu.ng

A. O. Ameen
e-mail: ameen.ao@unilorin.edu.ng

O. C. Abikoye
e-mail: abikoye.o@unilorin.edu.ng

S. A. Salihu
e-mail: salihu.sa@unilorin.edu.ng

M. Abdulraheem
e-mail: muyideen@unilorin.edu.ng

I. D. Oladipo
e-mail: odidowu@unilorin.edu.ng

J. B. Awotunde
e-mail: awotunde.jb@unilorin.edu.ng

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_9

Since MRS needs interaction between constituent robots and IoT provides a ready medium for interaction, it is only natural for the two technologies to be merged in order to form a powerful computational and communication platform for executing robotic task both in programmable form and autonomously. This merger is what birth IoRT.

The individual technology has found application in different domains with some level of intersection. Robots have been employed to perform important functions, such as human assistive operations, healthcare delivery, industrial processes, military supports, and rescue management, monitoring, and environmental and equipment regulation (Grieco et al., 2014; Batth et al., 2019; Simoens et al., 2018; Sethi & Sarangi, 2017; Thusabantu & Vadivu, 2019; Scilimati et al., 2017). Also, IoT has been used in healthcare and smart environments such as homes, offices, and even factories. Thus, IoRT which is a combination of the two is applicable in all of these domains and provides a system that is smarter and more autonomous. Although this combination is an advancement to both worlds, the new breed comes with new challenges which need to be addressed in order to fully realize the potentials inherent in IoRT and even make it applicable in more wide and complex domains.

In this chapter, the two areas of IoT and Robotics are discussed. Then, IoRT is presented as a multidisciplinary technology that merges the two areas. The application of IoRT is presented, and some of the challenges that inhibits its full realization are discussed. The applicability of IoRT in educational libraries is also explored given that this area has not been given attention as others that are discussed in the chapter.

The chapter is organized as follows: Sections 2 and 3 present the concepts of IoT and Robotics, respectively. Section 4 discusses IoRT as a combination of IoT and Robotics. Section 5 presents some of the notable application of IoRT in the domain of smart environments (homes, offices, and industries), healthcare, and military including civil policing and rescue operations from disasters. Some of the challenges in the implementation of IoRT are discussed in Section 6, while Section 7 presents a proposal of the application of IoRT in library management. Section 8 concludes the chapter and highlights a further study on the empirical investigation of the use of IoRT in educational library.

2 Internet of Things

Internet of Things (IoT) is a paradigm which involves the interconnection of devices, often heterogeneous, with the capabilities of tracking, sensing, processing, and analyzing of information passed in the network. It offers a new environment in which sensors and other actuators seamlessly communicate with each other and their environment (Gubbi et al., 2013). The connected devices are smart and have sensing abilities and unique identification through the use of Radio Frequency Identification (RFID) technology. In RFID technology, electronic product codes are encoded in RFID tags which can be used to track smart objects in IoT.

IoT is basically based on the integration of sensors, RFID tags, and communicating technologies. Other components include embedded systems, mobile computing, cloud computing, low-price hardware, and even big data in order to provide computing functionality, data storage, and network connectivity for equipment that hitherto lacked them. One of the main capabilities of IoT include ability to collect and analyze data about the physical world and use the results for inform decision making and to alter the physical environment. Thus, it addresses traceability, visibility, and controllability of smart objects. IoT has had several applications which include environmental monitoring, healthcare service, manufacturing, inventory, and production management.

There are several IoT architectures which differ in the number of layers as a result of the level of granularity depicted in the architecture. At the early stage of IoT development, a three-layer architecture depicted in Fig. 1 suffices. The three layers are the perception layer, the

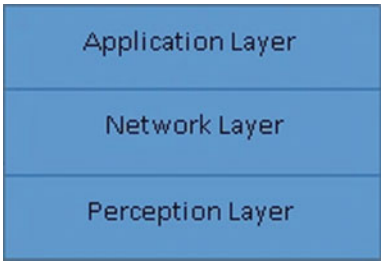


Fig. 1 Three-layer IoT architecture

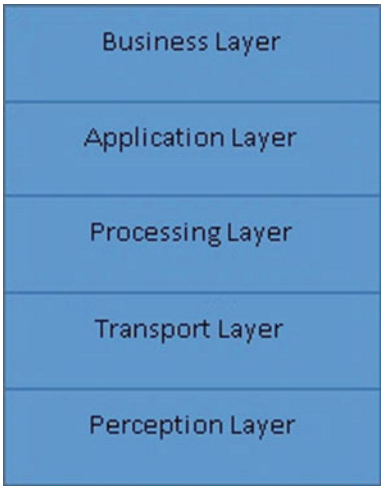


Fig. 2 Five-layer IoT architecture

Table 1 IoT architecture layers and their functions

S. No.	Layer	Function
1	Perception	This is the physical layer that comprises sensors that perceive and gather information from the IoT environment, i.e., senses available smart objects
2	Network	This layer is responsible for connecting smart objects, transmitting sensor data/information, and connecting to network devices and servers
3	Transport	Comprises of networks that transmit sensor data from the perception devices to the processing layer devices. These networks include Bluetooth, RFID, NFC, 3G, 4G, and even LAN
4	Processing	This layer is responsible for storing, processing, and analyzing. This layer uses technologies such as database, cloud computing, mobile computing, and big data analytics
5	Application	Defines the various areas in which IoT can be applied and responsible for delivering application specific services to users
6	Business	This layer manages the application models, business models, and user security

network layer, and the application layer. A more comprehensive architecture is depicted in Fig. 2. Table 1 presents the descriptions of the layers (Sethi & Sarangi, 2017).

3 Robotics

Robotics is a multidisciplinary field that comprises majorly science, engineering, and technology geared toward the development of mechanical robots that efficiently and effectively perform most human actions. The goal of robotics is to design intelligent machines that can assist humans in day-to-day activities and for engineering processes. Advancement in technology provided the platform for modeling robots to execute tasks that mostly require precision and that are repetitive and tedious in nature. There are several operations and places that robots can be applied, and these include firefighting, manufacturing plants, surgical assistance, delivery services, cleaning, heavy object lifting and movement, searching and information gathering, and detecting objects such as landmines in warfronts. Thus, some of the popular areas where robotics are useful are manufacturing, logistics, homes, travels, and healthcare.

The advent of artificial intelligence (AI) has seen the development of intelligent robots that can learn from their environment while performing their tasks. Some of the notable application of AI robotics is in the development of drones that aid emergency response operations, law enforcement, and even search and rescue operation. They (drones) can be used to collect information such as source of wild fire outbreak, location of kidnappers and hostages, or the level of impact of the damages caused by disaster situations. Roomba is a vacuum cleaner robot that can adapt to its given environment by mapping it out while cleaning floors. Robots can also be made to adapt to working with humans, taught by humans by way of moving them around during the tasks, and they can adjust the amount of force applied to handling objects in their environment.

Besides manufacturing, robots have found applications in other sectors such as security, education, entertainment, and healthcare. One of the common attributes of robotics that has contributed to its applicability in these sectors is that they are programmable to perform their task, thus making them to be easily amenable to perform different task with little resemblance. Other common attributes of robots include: They consist of some level of mechanical construction which is determined by the nature of the tasks for which they are designed, and they also consist of electrical component as well.

Mostly, the robotic system consists of three components which are: control, actuation, and sensors. This is depicted in Fig. 3.

As shown in Fig. 3, the control is responsible for the connection of action into perception in an intelligent manner. The actuation has the capability to exert an action, in terms of locomotion and manipulation. It also provides and

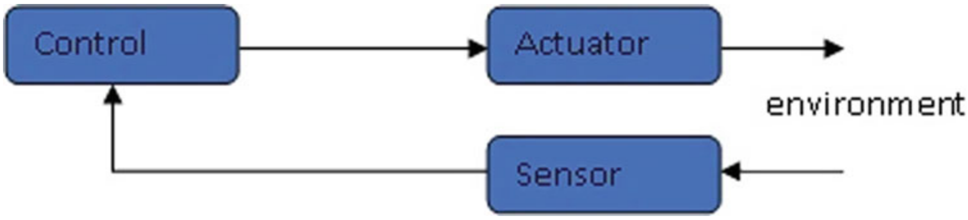


Fig. 3 Components of robotics

animates the mechanical system of the robots. The sensory is responsible for perception, acquiring of data on the internal status of the mechanical system, and the external status of the environment (Siciliano, 2010).

Types of Robots

Robots come in different shapes and sizes depending on the nature of the task they are designed to carry out and the environment in which they will operate. Some robots usually mimic the structure of the original entity, most often humans or their parts, which carry out the task the robots are designed to perform as a substitute. For instance, car assembling robots are modeled after human arms to carry out tasks such as welding and screwing of car parts during manufacturing. Robots can be grouped into two main categories (Tzafestas, 2018): the service robots which are designed to render assistive service to users in an indoor environment such as homes and offices; and the field robots which are designed to operate outdoor in field where the environment is unstructured and have less constrained. The field robots are further classified into marine robots designed to operate under water; ground robots, operate on ground surface; and ariel robots design to fly and operate in the airspace. Another classification of robots includes the following five categories:

Preprogrammed robots: These are robots for controlled environments and monotonous task. Details of the tasks and environment are foreknown comprehensively, and they are tailored to work as programmed. A typical example is the mechanical arm on automotive assembling line. This arm mimics the human arm, and it performs the task more efficiently and repetitively without getting fatigued (Gawli et al., 2017).

Humanoid robots: As the name implies, they are robots that are physically and/or behaviorally human like. A typical example of this category is Sophia and Atlas of Hanson Robotics and Boston Dynamic, respectively.

Autonomous robots: These are robots that operate independently of humans, i.e., they require no human supervision, they are intelligent enough to control themselves. An example if Roomba, the vacuum cleaner robot that uses sensors for roaming and mapping out its environment while cleaning.

Tele-operated robots: Unlike the autonomous robots, tele-operated robots are controlled by humans. They are often designed to operate in complex environments and difficult circumstances. Typical examples are drones used to detect landmines in battlefield, robots for performing surgery, and underwater robots for fixing pipe leakages.

Augmented robots: These are robots used to complement or replace the human capabilities that may be deficient or lost. Some typical examples are prosthetic limbs for the physically challenged and exoskeleton robots used for lifting heavy objects.

4 Internet of Robotic Things

As it can be guessed, Internet of Robotic Things (IoRT) sometimes referred to as Internet of Things Robotic is a merging of the concept of IoT and Robotics in which IoT serves as the smart context in which robots operate thereby making robots smarter than they ordinarily were in carrying out designated tasks. This integration of robots into smart environments makes the robot to be aware of their environment and communicate with other things besides their fellow robots. Given this new context awareness and the autonomous capability of some robots, they become more knowledgeable and smart in carrying out more complex tasks (Simoens et al., 2018).

Although there is no universal definition of IoRT yet, some studies have attempted to provide definitions. A comprehensive definition is given by Ray (2016) as follows:

> A global infrastructure for the information society enabling advanced robotic services by interconnecting robotic things based on, existing and evolving, interoperable information and communication technologies where cloud computing, cloud storage, and other existing Internet technologies are centered around the benefits of the converged cloud infrastructure and shared services that allows robots to take benefit from the powerful computational, storage, and communications resources of modern data centers attached with the clouds, while removing overheads for maintenance and updates, and enhancing independence on the custom cloud-based middleware platforms, entailing additional power requirements which may reduce the operating duration and constrain robot mobility by covering cloud data transfer rates to offload tasks without hard real time requirements.

IoRT Architecture

Studies in IoRT have attempted to give a high-level architectural view of the landscape of IoRT. Figure 9.4 depicts the landscape of IoRT, showing the specific roles of robots and IoT, their main functions, required technologies. and applications to function and application domain (Afanasyev, 2019).

As shown in Fig. 4, robots in IoRT are the intelligent agents that carry out actions sensed and communicated via the IoT component of the system. The robots need to possess some abilities to be able to carry out their vital role in the system. Simoens et al. (2018) discussed the key abilities of the robots which include both the basic abilities of robots and a set of high-level abilities that make the robots to be smart in performing their roles. The basic abilities include: perception ability, to be able to collect environmental information for awareness and location within its environment; motion ability, to be able to move from one point to another within its usually dynamic environment; and manipulation ability, to be able to process information and change its environment as and when required. Other abilities that are high level include decisional autonomy ability, to be

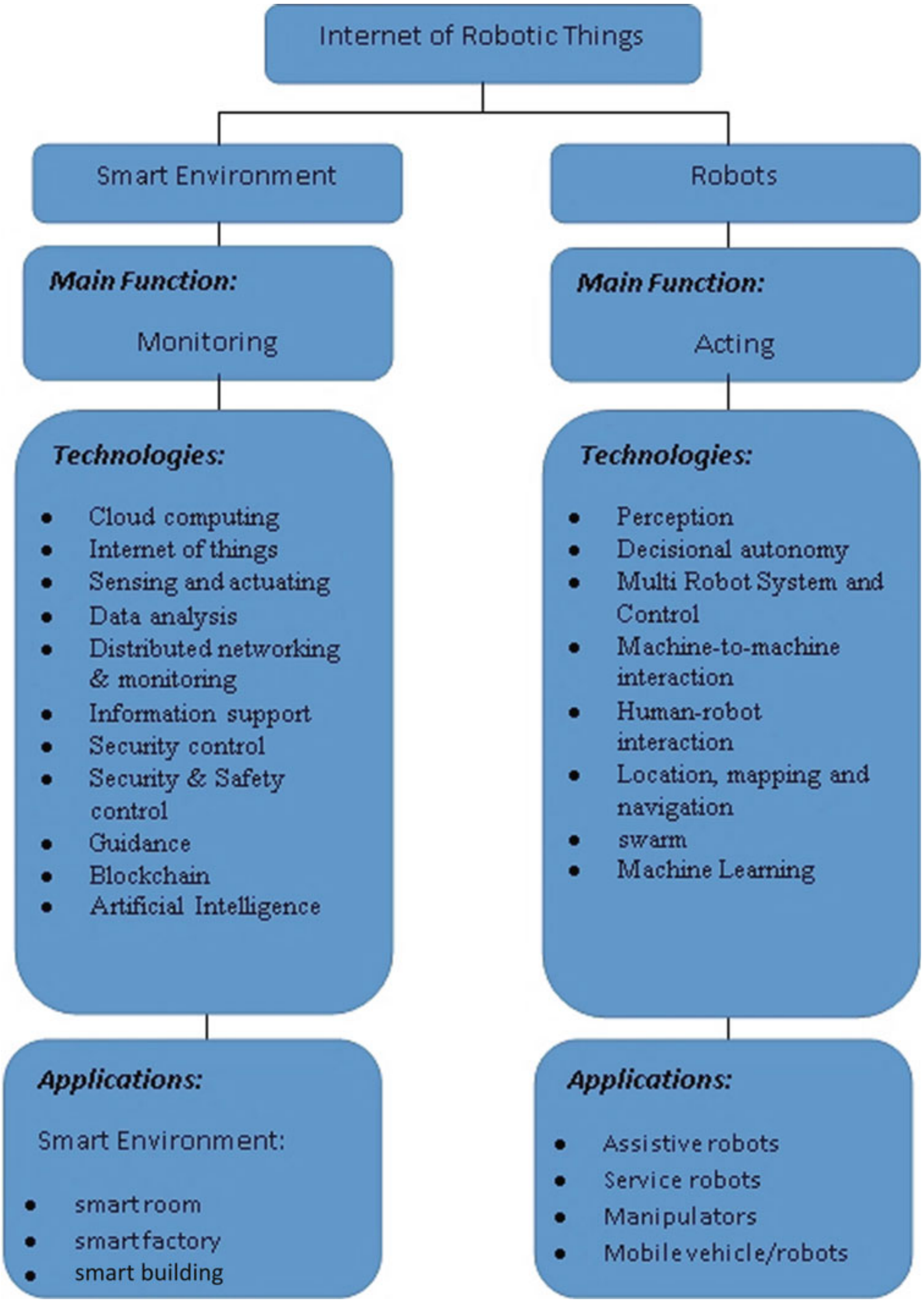


Fig. 4 IoRT landscape. *Source* Afanasyev et al. (2019)

able to take decisions independently and intelligently; interaction ability, to communicate with other "things" in its environment to ensure the smooth execution of their task: for instance to avoid collision with other object, the robot needs to map out the environment and identify the location of other objects; cognitive ability for learning and reasoning using the perceived data/information collected from the environment.

As a system, the features that the IoRT should have are configurability and dependability. In terms of configurability, the system should be amenable to carry out different but related tasks, i.e., it should be adaptable for different environments. In terms of dependability, the system should be resilient, and its failure rate should be tolerable. Security is a key aspect to be considered in IoRT since it inherits the risk associated with the Internet–network hacking. Component integrity, authentication, and authorization must be ensured using strong cryptography models to prevent hackers from intruding into IoRT networks to cause malicious acts.

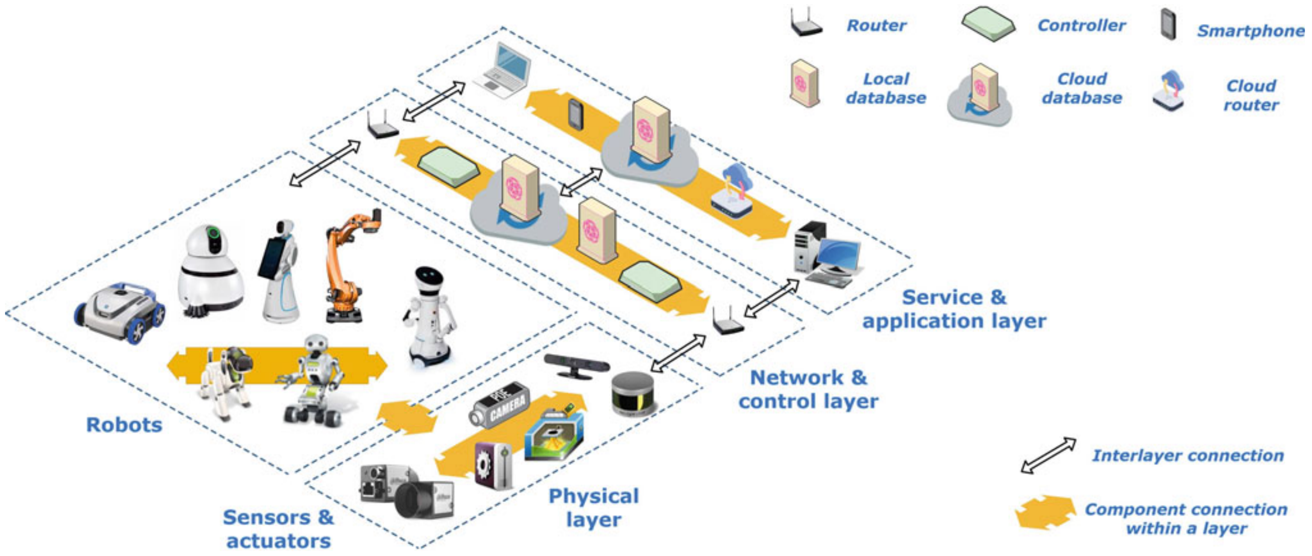


Fig. 5 IoRT architecture (Excerpt from Afanasyev et al. (2019))

Table 2 Roles of IoRT architecture layers

Layer	Role
Physical	This comprises the smart robots, sensors and actuators. The robots are intelligent agents that connect and communicate with other components, sensors are the hardware for perceiving the environment while actuators are the devices that implement intended actions such as switching components on/off, lifting objects, etc.
Network and control	This layer is saddled with the responsibility of interconnecting and managing the things in the environment using various network protocols and devices such as TCP/IP, Routers, Bluetooth, Wi-Fi, WLAN, RFID, storage medium and devices
Service and application	This layer provides the feature for programming and configuring the IoRT system including the robots, sensors and actuators as well as controls

Also, (Afanasyev et al., 2019) proposed a three-layer IoRT architecture that comprises the physical layer, network and control layer, and the service and application layer. Figure 5 and Table 2 present the three layers and their roles, respectively.

In Ray (2016), a more detailed architecture for IoRT with five layers was presented. Figure 6 presents a view of the layer while Table 3 gives the role of the layers.

Another architecture layer was presented by Hardmeier (2013). It is an expanded communication protocol for IoRT application that depicts a five-layer protocol and the associated technologies for each of the layers. Figure 7 depicts this IoT protocol stack layer for IoRT applications.

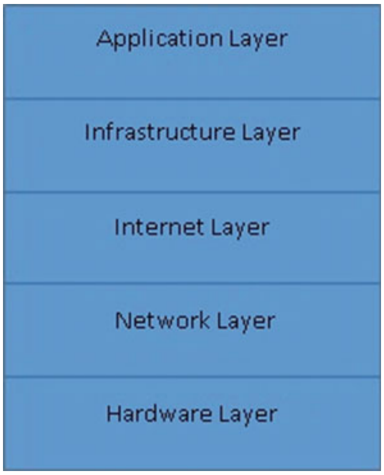


Fig. 6 Five-layer IoRT architecture (Ray, 2016)

5 Applications of IoT Robotics

IoRT has found applicability in various domains. It is applicable in most of the areas where robots have been used and areas where IoT have also been applied. Application of IoRT creates smart environments which include smart home, smart office, smart factory, and smart city. Other notable areas where IoRT are been applied are healthcare (especially telemedicine and eHealth), industry assembly, policing (search and rescue), and military. Grieco et al. (2014) depicted an application framework showing how IoRT can be utilized as shown in Fig. 8.

Table 3 Five-layer IoRT architecture

Layer	Description
Hardware	This is the lowest layer of abstract that comprises of the physical objects such as the robots, sensors, actuators, and even smart phones
Network	This level of abstraction describes the various network connectivity that can be leveraged for the connection of the robotic things. This includes: telecommunication networks such as 3G and 4G, Bluetooth, NFC, WiMAX, and Z-wave
Internet	This layer defines the Internet connectivity required for IoRT, especially the communication protocols that are suitable for robotic communication such as IPv6, UDP, MQTT, CoAP, XMPP, uIP, DTLS, AMQP, LLAP, and DDS
Infrastructure	This layer is considered the most vital, providing some cloud-based computational facilities and middleware for the operation of IoRT. These infrastructures include machine-to-machine-to-actuator cloud platform support, robotic cloud platform support, IoT cloud infrastructure, IoT business cloud services, and big data services
Application	This layer is the top most layer and provides the abstraction for configuring and programming the IoRT system to meet user-specific needs and requirements

Source Ray (2016)

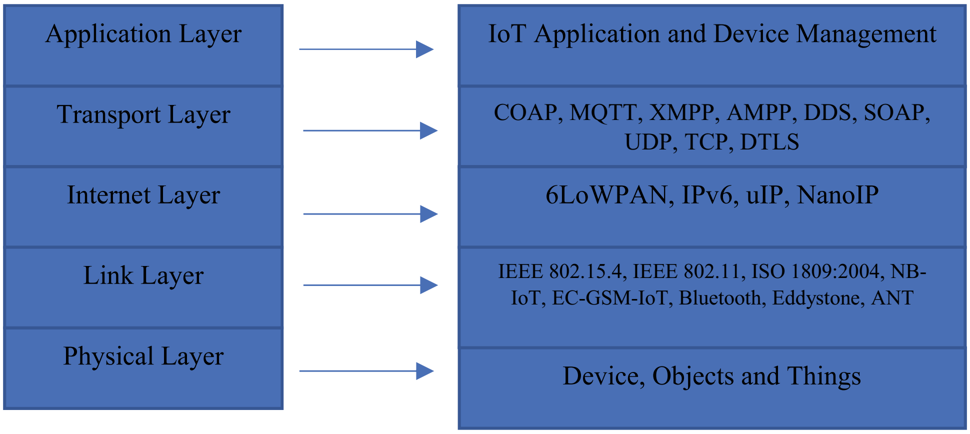


Fig. 7 IoT communication protocol for IoRT application

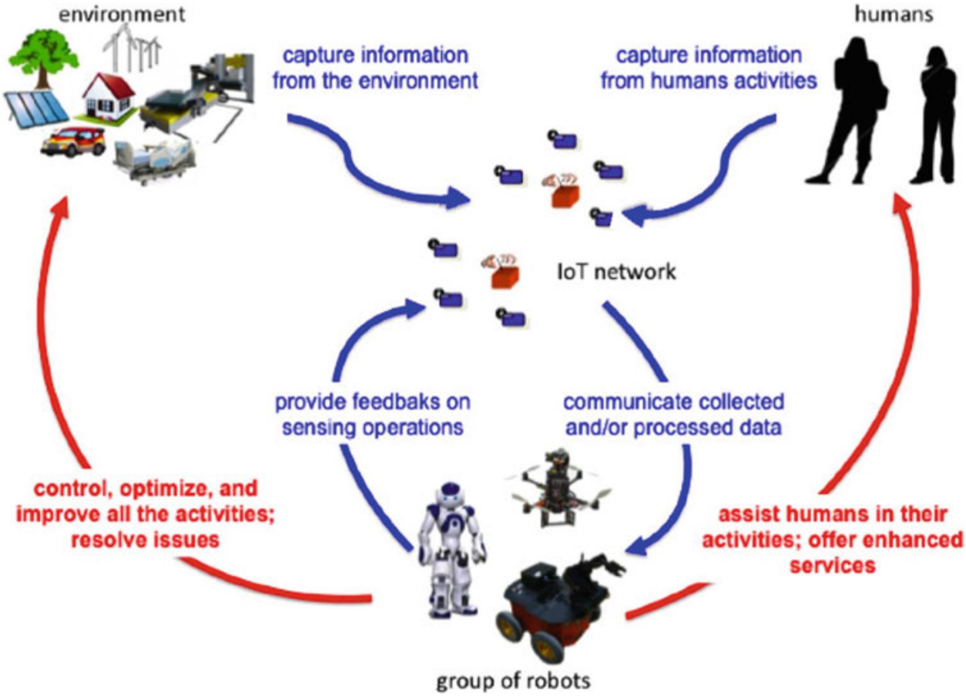


Fig. 8 An application framework of IoRT. *Source* Grieco et al. (2014)

Fig. 9 AppBot riley home security and monitoring robot

"AppBot" Can Keep Your House Safe from Intruders

Robot can moving room to room while monitoring.

Control robot and view screen at anywhere through internet access.

All round View with no blind spots

Unlike any other home security devices, AppBot is the first robotic home security camera that can actually see, hear, sense, and track moving objects, all while communicating you.

5.1 Smart Environment and Industry

Smart home and office include the use of IoT and now IoRT for efficiently performing home and office task such as environmental temperature and humidity regulation, household chores, scheduling and reminder system, and even personal health and remote patient monitoring. Also, smart robots can serve as assistants in office meeting scheduling and logistics. Smart factory can include smart robots that control and monitor manufacturing processes via M2M communications and coordination, performing task such as environmental condition monitoring and regulation, heavy object lifting, location and mapping, and even complex and safety-critical tasks that otherwise are risky for humans.

Smart homes as relates to IoRT entails the engagement of robots in home management to carry out domestic tasks such as cleaning, washing, monitoring, and control. Roomba is a robot designed to clean indoor environment. AppBot Riley, depicted in Fig. 9, is a typical monitoring robot that can be used for both indoor and outdoor home security (The Prism Group, 2020); to monitor the activities of children indoor. The robot is equipment with camera for live streaming and can move about within its environment.

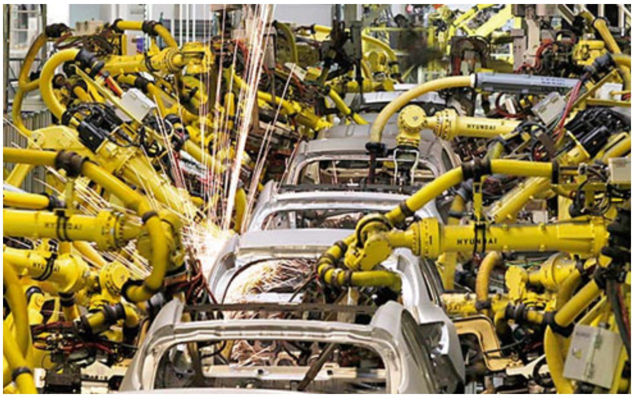


Fig. 10 Robots assembling cars in Chennai plant

Manufacturing industry has seen the application of robots to perform tasks that are energy-intensive, risky, and require high level of precision and accuracy. A typical example is the assembling arm used in car manufacturing, see Fig. 10. Making the robots in the industry smart requires the IoT technology among others. Other key technology needed also include M2M for communication between robots without having to consult a central location or server. With smart objects and sensing devices in the environment, robots can be made to perform even more complex tasks and in a cooperative manner involving more than one robot at a time, working in consensus to carryout operations without making conflicting decision and actions. The areas where IoRT is applicable in industries include:

1. Autonomous movement of industry equipment when needed
2. Industry environmental condition measurement and regulation (such as furnance temperature measurement and

control, detection and possible elimination of toxic chemical in the air in facility areas)
3. Management of facility energy requirements such as electricity
4. Access control management for safety and security
5. Prediction of failure and disaster to mitigate them before they occur and management of disastrous situation if they occur.

Grieco et al. (2014) presented a comprehensive scenario of the applicability of IoRT in the airport operation and management; highlighting the technological and computational requirements for the implementation of an airport IoRT—see Fig. 11. Robots in the IoT context can be made to man or assist humans in airport check-in, boarding, luggage, security, and even emergency situation management.

Interestingly, the application of IoT-aided robots in the food processing and production industry for production of health food is being considered. The production of special type of food for persons with, say, diabetes and heart disease was explored by Bader and Rahimifard (2020).

5.2 Healthcare

Healthcare delivery is one of the major domains where IoT and Robots are being applied to assist caregivers or as caregivers to efficiently deliver timely and effective services. The inclusion of robots into telemedicine, eHealth, and mHealth technology increases capacity to deliver healthcare to patients both in-house and remotely to places where needed. Figure 12 depicts some applications of robotics in healthcare delivery.

The figure, respectively, shows a robot used to assist patients with motor problem, robotic arm for performing surgical operations, and Zora, a caregiver robot that can be used in nursing homes (Adams et al., 2018). These robots and more with IoT will tremendously enhance and increase the healthcare delivery capacity of health worker both remotely and in-house. Some of the areas where IoRT is applicable in healthcare are:

1. Remote patient monitoring (RPM)
2. Assisting patients with motor disabilities to perform recovery exercises

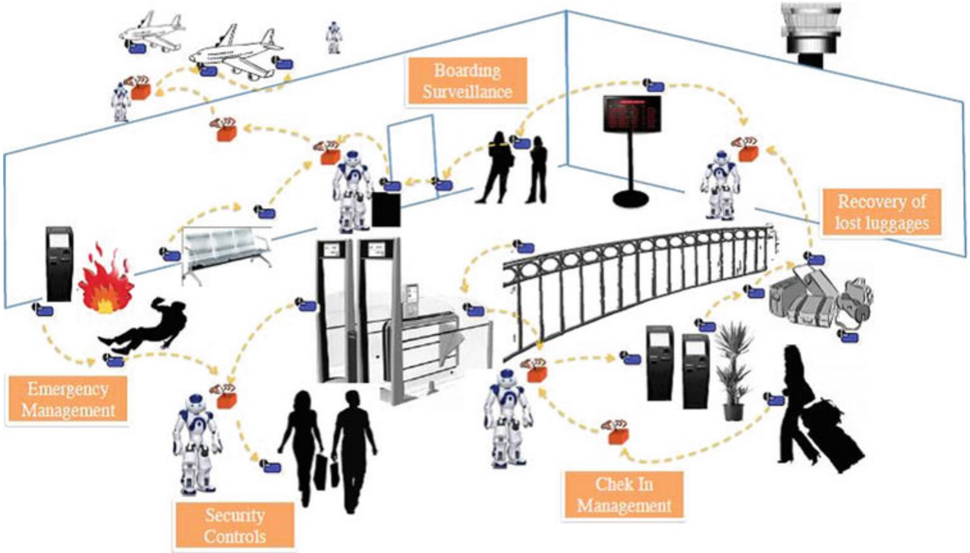


Fig. 11 Smart airport with IoT-aided robots. *Source* Grieco et al. (2014)

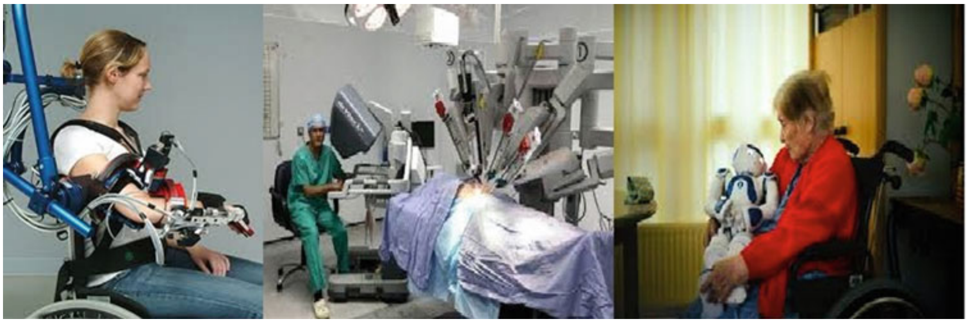


Fig. 12 Robotics healthcare

Fig. 13 BigDog designed by Boston dynamics

3. Management of drug storage, discovery, movement, and delivery as well as its administration to patients.
4. Emergency assistance
5. Hospital environmental condition and medical equipment monitoring and regulation
6. Management of safety and security within hospitals.

Networking and mobile computing technology provides a good medium for the implementation of healthcare IoRT. The use of wireless body area network (WBAN), RFID, Bluetooth, etc., as well as mobile technology (3G, 4G, and 5G) and mobile devices create connections for robots for remote sensing and communication, i.e., robots can connect to other "things," receive and send data to one another, process the data, and take actions based on acquired information using these technologies.

Aside accessibility to healthcare, efficiency and timeliness in healthcare delivery, IoRT will also be highly useful in pandemic situations such as the COVID-19. Robots can be used to remotely and virtually attend to patients to ensure physical distance to avoid physical contact in order to fight the spread of infectious diseases.

5.3 Military and Policing

IoT and Robotics as individual technology have been used in the military ecosystem (Ha et al., 2019) and security in general. For instance, IoT are applied for detection and prevention of intrusion, detecting presence of chemical, biological, and explosive devices. Yushi et al. (2012) presented a high-level Military IoT (MIoT) architecture. The architecture comprises a sensing layer that captures data/information from human, materials, equipment, and devices in military environment; and information layer that shares collected information among military personnel, equipment, and application. On the other hand, robots have been intensively used in military operations and experiments. One of the notable applications is in unmanned vehicles such as in unmanned ground vehicle (UGV), unmanned surface vehicle (USV), unmanned aerial vehicle (UAV), and unmanned underwater vehicle (UUV). Building intelligence into robots has seen the design and development of BigDog, a four-legged robot that can operate in complex and rough environment carrying military equipment and highly resilient to noise—Fig. 13. Military drones are unmanned and tele-operated form of robots that are used in spying operations and even enemy targeting and execution. These robots have found use in military and policing operations such as area (e.g., border) surveillance and mine detection on combat fields.

Merging the capabilities of IoT and Robotics into IoRT which makes the robots to be more knowledgeable and intelligent greatly enhances the application of these technologies in the military ecosystem. Thus, based on the respective application of these two technologies, IoRT are applicable in the following areas of military operations:

1. autonomous detection of harmful chemicals and biological weapons and ground mines; and safe storage and deployment of nuclear weapons,
2. autonomous control of military vehicles and aircrafts with little or no human intervention,
3. provide assistance in both policing and war operations,
4. securing military facilities by providing role-based access control (RBAC) and restriction to sensitive and risky environments.

Besides the high-end military application of IoRT, it is also applied in civil policing and rescue operations. Police–civilian altercation that often lead to shooting and killing of either police officers or civilians can be avoided by deploying IoT-aided robots to interact with civilians at road checkpoints and home thereby eliminating the chances for shooting and/or killings due to provocations. Also, safety at mining sites can be assessed by deploying robots to examine them before engaging humans to perform mining operations. In case of disaster, robots can also carry out rescue operations.

Fig. 14 Application of IoRT in educational library

6 Challenges in Implementing IoRT

Some of the key areas where research is focused in the full actualization of IoRT application include interoperability in heterogeneous context and distributed computing environment; energy usage optimization (Rajendran & Lourde, 2016); autonomy of robots and things using artificial intelligence (AI) (Alsamhi et al., 2019)—specifically usage of machine learning (ML) algorithms in autonomous decision making by robots; security using measures such as cryptographic algorithms for confidentiality, authentication, and authorization, and integrity of IoRT components to prevent intrusion, identity theft, and other cyber security attacks which are inherited from the Internet aspect of the IoRT framework.

M2M and human–robot interaction (HRI) have attained a mature stage where they can be applied to solve the problem of communication between "things" in a distributed environment. Data sharing in IoRT or its constituent technologies is on anytime basis and has to be timely. Edge computing and big data are considerable in handling and sharing data in complex communication (Thusabantu & Vadivu, 2019). M2M interaction also requires some level of cognitive autonomy of the robots and other things in the IoRT environment which can be achieved using AI/ML.

IoRT environment must be secured against hacking—cyber security threats from the connectivity component of the IoRT—since networking forms the backbone for the IoRT operation and it (networking is susceptible to cyber attacks). The robots and other "things" in the IoRT environment must be authenticated and authorized to carry out functions within the IoRT settings, and the communication links must be protected from eavesdropping and hijacking by using point to point secure communication protocols. Some of the measures that are amenable to IoRT security are network security digital certificate and signature but must be adapted to function in a distributed environment.

In the adoption and/or adaptation of existing technologies for the implementation of IoRT, computational complexity in terms of time and space must be considered in order to avoid problems associated with latency delay in processing and communication (Micoli, 2019). Robot and things are limited in both computational speed and memory, thus computational algorithms and data structures that are efficient in time and space usage must be used in building the IoRT environment.

7 IoRT in Libraries

Educational or academic library is one notable area where the application of IoRT is possible but has not be considered like other smart environment discussed in Sect. 5.1. IoT application prototypes and models have been proposed (Wójcik, 2016; Brian et al., 2014), and robots have been considered for use in libraries (Pujari & Deosarkar, 2017), but the merging of IoT and robotics has provided the opportunity to further make libraries smatter by engaging smart robots in an autonomous manner. Library catalog and collection stack management in physical libraries is a very vital part of the tasks that librarians do. In the context of IoRT, robots can be made to autonomously assist librarians in performing these tasks; patrons can interact with robots to borrow and return print documents (books). With sensing and actuation, IoRT can be applied in library environmental condition and regulation. Also, using the Internet, remote communication between libraries can be implemented. Figure 14 presents an architectural view of a smart library environment using IoRT.

8 Conclusion

IoRT is a technology that has come to revolutionize industrial processes, healthcare delivery, military, security, and most ways of human life and activities. A world where autonomous robots and every vital objects and things can communicate both remotely and in-house to carry out majority of the tasks been performed by human and standalone machines is envisaged. IoRT is being applied in developing smart homes, offices, industries (Industry 4.0), and military operations. Although, it is an improvement on IoT and robotics as individual context, IoRT also comes with technological challenges. Efficient algorithms and computational models need to be in place to ensure the autonomy of robots and the security of the network and communication in IoRT. The algorithms and computational models must be distributive to be usable in the IoRT environment; centralized computation and communication will pose serious problems in the application of IoRT for the future. As future direction, the application of IoRT in libraries will be explored further with a view to implementing IoRT in education library.

References

Adams, S., Peltria, E., & Kostyukov, D. (2018). Meet Zora, the robot caregiver, *The New York Times—Technology*. (Online). Available: https://www.nytimes.com/interactive/2018/11/23/technology/robot-nurse-zora.html.

Afanasyev, I., et al. (2019). Towards the internet of robotic things: Analysis, architecture, components and challenges. In *Proceedings of 2019 12th International Conference on Developments in eSystems Engineering (DeSE)* (Vol. October-20, pp. 3–8).

Alsamhi, S. H., et al. (2019). Survey on artificial intelligence based techniques for emerging robotic communication. *Telecommunication System, 72*(3), 483–503.

Bader, F., & Rahimifard, S. (2020). A methodology for the selection of industrial robots in food handling. *Innovative Food Science & Emerging Technologies, 64*(102379).

Batth, R. S., Nayyar, A., & A. Nagpal, A. (2019). Internet of robotic things: driving intelligent robotics of future—concept, architecture, applications and technologies. In *2018 4th International Conference on Computing Sciences (ICCS)* (pp. 151–160).

Brian, A. L. A., Arockiam, L., & Malarchelvi, P. D. S. K. (2014). An IOT based secured smart library system with NFC based book tracking. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11*(5).

Gawli, K., Karande, P., Belose, P., Bhadirke, T., Bhargava, A., & College, A. (2017). Internet of Things (IOT) based robotic ARM. 757–759.

Grieco, L. A., et al. (2014). IoT-aided robotics applications: Technological implications, target domains and open issues. *Computer Communications, 54,* 32–47.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Ha, Q., Yen, L., & Balaguer, C. (2019). Robotic autonomous systems for earthmoving in military applications. *Automation in Construction, 107*.

Hardmeier, C. (2013). Internet of robotic things—converging sensing/actuating, hyperconnectivity, artificial. (Vol. 2013, No. August, pp. 193–198).

Micoli, G., et al. (2019). ASAP : A decentralized slot reservation policy for dynamic 6TiSCH networks in industrial IoT (1), 4–9.

Pujari, T. S., & Deosarkar, S. B. (2017). Design of intelligent and robotic library system. In *Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on*, 2017, pp. 1903–1908.

Rajendran, S., & Lourde, M. (2016). Ab-initio study on FinFETs and their application in IoT aided robotics. 38–42.

Ray, P. P. (2016). Internet of robotic things: concept, technologies, and challenges. *IEEE Access, 4,* 9489–9500.

Scilimati, V., et al. (2017). Industrial internet of things at work: a case study analysis in robotic-aided environmental monitoring. *IET Wireless Sensor Systems, 7*(5), 155–162.

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering, 2017,* 1–25.

Siciliano, B., et al. (2010). *Robotics: Modelling, Planning and Control*. Springer Science & Business Media, pp. 22–23.

Simoens, P., et al. (2016). Internet of robotic things: Context-Aware and personalized interventions of assistive social robots (short paper). In *Proceedings—2016 5th IEEE Int. Conf. Cloud Networking, CloudNet 2016* (pp. 204–207).

Simoens, P., Dragone, M., & Saffiotti, A. (2018). The internet of robotic things: A review of concept, added value and applications. *International Journal of Advanced Robotic Systems, 15*(1), 1–11.

The Prism Group. (2020). Appbot-LINK smart home security robot. Accessed July 14, 2020. (Online). Available: https://iot.do/devices/appbot-security-robot.

Thusabantu, N. F., & Vadivu, G. (2019). Adoption of big data streaming techniques for simultaneous localization and mapping (SLAM) in IoT-aided robotics devices. *Cognitive Informatics and Soft Computing* 315–320.

Tzafestas, S. G. (2018). Synergy of IoT and AI in modern society: the robotics and automation case. *Robotics & Automation Engineering Journal, 3*(5).

Vermesan, O., Bröring, A., Tragos, E., Serrano, M., & Bacciu, D. (2017). Internet of robotic things: converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT Platforms. In O. Vermesan, & J. Bacquet (Eds.), *Cognitive Hyperconnected Digital Transformation Internet Things Intelligence Evolution* (pp. 97–155).

Whitesides, G. M. (2018). Soft robotics. *Angewandte Chemie International Edition, 57*(16), 4258–4273.

Wójcik, M. (2016). Internet of Things–potential for libraries. *Library Hi Tech, 34*(2), 404–420.

Yushi, L., Fei, J., & Hui, Y. (2012). Study on application modes of military internet of things (miot). In *IEEE International Conference on Computer Science and Automation Engineering (CSAE)* (Vol. 3, pp. 630–634).

Applications of GPUs for Signal Processing Algorithms: A Case Study on Design Choices for Cyber-Physical Systems

Neelesh Ranjan Srivastava and Vikas Mittal

Abstract

Nowadays, signal processing algorithms are simulated generally using MATLAB. Their hardware implementation requires either application-specific IC (ASICs) or system on chip (SoCs). But there are severe constraints on producing such chips. Therefore, hardware implementation on graphical processing unit (GPUs) or field programmable gate array (FPGA) can provide the answer to the problem. Signal processing involves mathematical calculations in the form of algorithms, which are required to be implemented finally as stand-alone hardware to be used as a system. Recently, GPUs have increasingly being used for hardware implementation of signal processing algorithms. This is because they can be programmed easily with the help of open-source coding languages like Python, CUDA, or OpenCL providing cost benefits in terms of lower costs and generic programming. Also, they possess, in general, a greater number of cores as compared to ASICs or SoCs making GPUs multi-application platforms that can solve the problem of the lower yield factor of the ASICs. They are also better than ASICs and SoCs in terms of performance since it has a dedicated processor to handle 2D and 3D graphics, which comprises of polygons and polygonal transformations involving computationally dearer multiple floating-point operations. Hence, more complex signal analysis can be performed using them. Additionally, the massively parallel architecture of GPUs further enhances their high computing performance. There exist many GPU-accelerated applications that provide an easy way to high-performance computing (HPC). In light of the above discussion, this chapter intends to inform and help readers know properly about the hardware implementations of different signal processing algorithms, by showcasing appropriate hardware platforms and different open-source coding languages along with their implementation methodologies. Therefore, they will be able to appreciate the difference between hardware implementations using ASICs/SoCs or GPUs/FPGAs. As GPUs or FPGAs take a faster time-to-market approach, as no layout, masks, or other steps are required for the manufacturing, they possess a simpler design cycle and the most important, the feature of field reprogram ability.

Keywords

Signal processing algorithms • Hardware implementations • FPGA • Hardware platforms • GPU • CPU

1 Introduction

In this chapter, signal processing and related algorithms have been discussed along with their hardware implementations for real-time analysis with appropriate inputs to achieve the desired outputs. Presently, hardware implementation of signal processing algorithms is carried out conventionally using two steps, viz. simulation using MATLAB followed by hardware implementation over application-specific integrated circuits (ASICs), system on chip (SoC), or field programmable gate arrays (FPGAs) using VHDL coding (Kiran et al., 2008). The coding and implementations over the ASIC or FPGA (Shi et al., 2018).

The stepwise process of FPGA implementation of signal processing algorithms is described below (Woods & Yi, 2017):

- Assign input signals in MATLAB environment for processing.

N. R. Srivastava (✉)
KIET Group of Institutions, Ghaziabad, Uttar Pradesh, India
e-mail: nr.srivastava@kiet.edu

V. Mittal
National Institute of Technology, Kurukshetra, Haryana, India
e-mail: vikasmittalkkr@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_10

- MATLAB converts signals to corresponding hexadecimal format in the form of a .hex file.
- This .hex file will be downloaded to Avnet Board SRAM with the help of PCI Utility.
- HyperTerminal issues the instructions to start the filtering process.
- PCI utility reads results from SRAM.
- MATLAB checks the parse .hex file to check results.

This chapter discusses the hardware implementation of signal processing algorithms using a stand-alone system that can use a single coding language for defining both processes of simulation and hardware. This can be served best using a graphics processing unit (GPU) due to their typical design implementing both the above processes on a single chip in a stand-alone system having a hardware-implemented signal processing algorithm (Andrade & Crnkovic, 2018).

This stand-alone system can be reconfigured for different algorithms making it suitable for the implementation of different algorithms. Therefore, GPUs are a better option compared to ASICs or FPGAs due to many advantages such as GPUs have a wide application field with a mature ecosystem of applications and processes, they also offer an efficient platform for the new era applications, they are easily programmed as only single language can be used for all set of programming, as the GPUs can be implemented as stand-alone systems the development time will be very less and above all, as per the requirement of signal processing hardware implementations they are compatible to floating-point operations which are very much required for the signal processing operations.

This chapter will emphasize the study of different hardware platforms used for the signal processing algorithm implementations including different heterogeneous platforms along with FPGAs and GPUs (Dubey et al., 2020).

The hardware requirements for the implementations and the programming requirements for the implementation will have special attention. There will be a comparison done between all types of heterogeneous platforms to identify the best platform for the implementation purposes which comes out to be GPUs here, as per different programming and hardware aspects (Han et al., 2018).

The domains of signal processing and related algorithms are introduced in the next section.

2 Signal Processing

Nowadays, no one can imagine the situation without a mobile phone, analyzing and searching astronomical activities without the human presence or diagnosis of different diseases without the help of different diagnostic equipment and machines. Signal processing is a common denominator in all the above applications. The domain of signal processing is introduced next (Singh et al., 2020).

Technically, signal processing is a process to transform information containing into signals into a different form at the output based on an application. The transformation is an analog system for continuous-time input and output signals and is discrete or digital for input and output signals in the form of sequences of numbers.

Figure 1 represents the block diagram for the signal processing in the time domain and frequency domain. The detailed description for each of the blocks of Fig. 1 is defined as (Woods & Yi, 2017).

2.1 Analog Input

The analog input signal is a variable that can have multiple states. It can represent physical quantities like temperature, rate of flow, etc.

2.2 Analog Filter

These are the basic block of the signal processing process and can be defined as a combination of passive linear components like capacitor, inductor, and resistance. Analog filters are designed to operate on analog input signals.

2.3 Analog-to-Digital Converter (ADC)

ADCs are used to convert analog (continuous) signals into digital (discrete-time) signals.

2.4 DSP Algorithms

A DSP algorithm is defined as the stepwise procedure to process the digital signals with the help of mathematical calculations, for example, for audio processing, a DSP algorithm is a set of calculations to process digital audio signals (Han et al., 2018).

2.5 Display or Output

The display or output for the signal processing can be defined with two different aspects,

- Time domain display which represents the parameters concerning time.
- Frequency domain display which represents the frequency components defined over the frequency axis.

Fig. 1 Block diagram for signal processing

The signal processing theory is a vast field and has an impact on various applications like communications, bioengineering, environment monitoring, astronomy, oceanography, etc. In particular, the advances in the digital integrated circuit technology for computing evolutions enabled its further spread. These properly hardware-implemented systems allow advancements in the field of image, speech, video, audio, multi-rate processing along with digital controls and communication fields.

3 Signal Processing Algorithms

3.1 Introduction

In general, an algorithm is a stepwise set of instructions arranged to accomplish a specific task. The process can be simple as well as complex. The instructions can further be arranged as functions, which are small programs that can be referenced to or recalling application includes a library of different functions that are suitable for a particular application (Singh et al., 2020).

In several cases, there could be different ways or options to perform any specific task within the software. So, usually, it is to be defined by the users to create the most efficient algorithm (Han et al., 2018). An efficient algorithm means that the program can ensure short run time and the use of minimal resources (Raut & Gokhale, 2013). If an algorithm is not created perfectly, then developers optimize the algorithms with future software updates, i.e., a new version with faster processing and thus is more efficient. In Fig. 2, one can easily see the functions associated with a general algorithm (Woods & Yi, 2017).

For implementing an algorithm, the following need to be specified (Raut & Gokhale, 2013)

- **Inputs**
  The input values for any process must be specified clearly and well defined.
- **Outputs**
  The output values of any process must be specified clearly and well defined.
- **Definiteness**
  The algorithm must be clear and unambiguous as each step must be definite in all aspects which lead to one meaning or procedure at a time.
- **Effectiveness**
  The processes in any algorithm should be simple and practical so that this can be executed on available resources. The language of the algorithms must be defined as simple and can be implemented in any language.
- **Finiteness**
  The algorithms must be finite in the reference of procedures, i.e., there must not be some functions that yield any infinite processes (Fig. 3).

3.2 Signal Processing Algorithms

Different processes of signal processing are very complex, and calculations are done over an array of mathematical computations that are arranged in a definite set of instructions, known as signal processing algorithm. Some of the signals processing algorithms generally employed are (Han et al., 2018):

- **Fast Fourier transform (FFT)**
  The **fast Fourier transform** is a method that allows computing the DFT in O ($Nlog_N$) time. The basic idea of the FFT is to apply divide and conquer. We divide the coefficient vector of the polynomial into two vectors,

Fig. 2 Functions of an algorithm

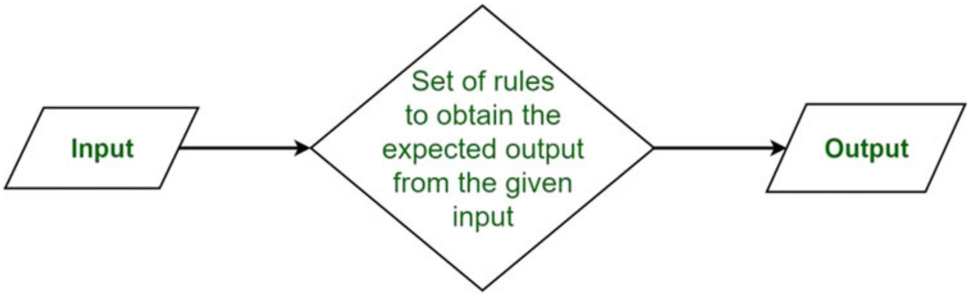
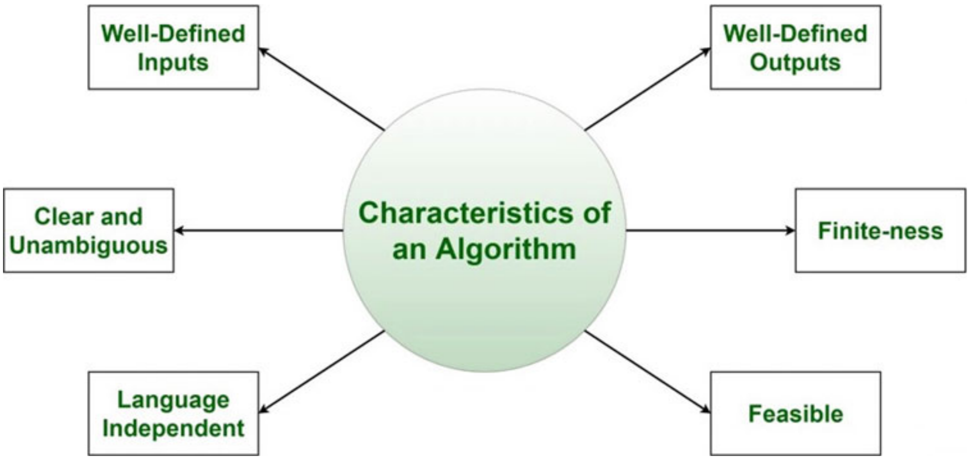


Fig. 3 Characteristics of an algorithm



recursively compute the DFT for each of them, and combine the results to compute the DFT of the complete polynomial (Rissa et al., 2002) (Fig. 4).

- Finite impulse response (FIR) filter algorithm
  A finite impulse response filter is a filter whose impulse response is of finite duration, as it settles to zero in finite time (Fig. 5).
- Infinite impulse response (IIR) filter algorithm
  IIR filter is a digital filter having feedback. Digital filter is also often described in the difference equation form, which defines the relationship between the output signal and the input signal (Fig. 6).
- Adaptive Filters Algorithm like Wiener and Kalman filters.
  The adaptive filter is a system with a linear filter that has a transfer function with variable parameters and a parameter to adjust those parameters with an optimization algorithm. Due to the complexity of the algorithms, all adaptive filters are digital filters.

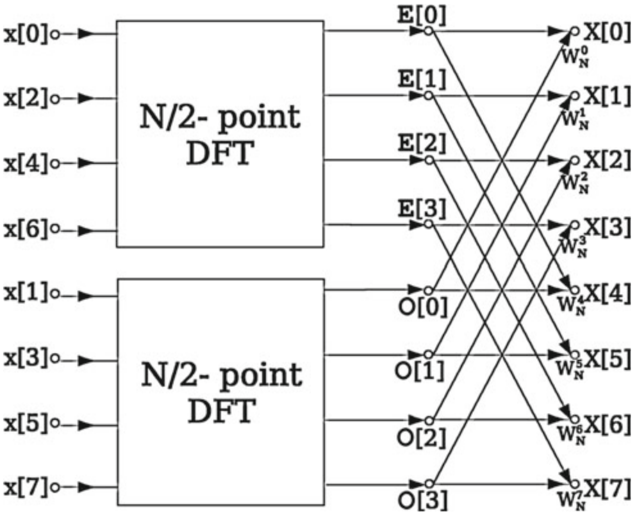


Fig. 4 An example of FFT algorithm

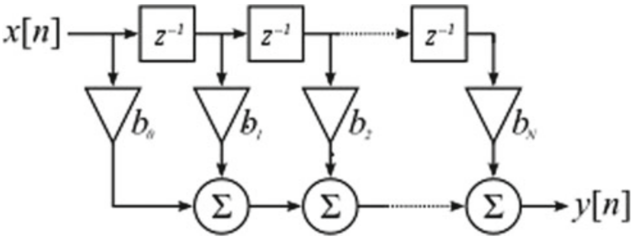


Fig. 5 An example of FIR filter algorithm

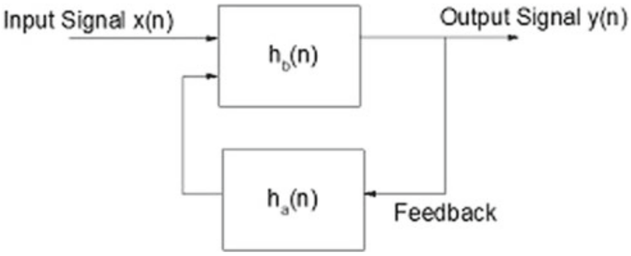


Fig. 6 An example of IIR filter algorithm

4 MATLAB Simulations of Algorithms

The simulation of a signal processing algorithm using a particular toolbox of MATLAB is described next.

Matrix Laboratory (MATLAB) is a multi-mode mathematical computing environment with an associated-programming language tool that is developed by MathWorks. Different MATLAB tools allow plotting functions, matrix analysis as well as implementations of different algorithms, user-interface formation, and interfacing of programs written in other languages. Although MATLAB (Kiran et al., 2008) is intended primarily for mathematical computing, an optional toolbox known as the MiPads engine is there that allows symbolic computing. An additional package, Simulink, adds graphical multi-domain simulation and model-based design for embedded systems. MATLAB users belong to various backgrounds in engineering, science, and economics.

MATLAB and Simulink are the basic tools or products which ease the signal processing techniques for synthesizing data and result in a unique workflow for embedded systems and other applications. These products can help the signal processing applications, as

- Prototyping, testing, and implementation of signal processing algorithms on computer systems, SoCs, FPGAs, and embedded processors.
- Design of algorithms for sensor, instrumentation, IoT, audio, etc.
- Measurement, acquirement, and analyzing signals from different sources.

With the help of MATLAB signal processing tools, various operations for synthesizing data sources can be easily accomplished such as (Apolinário and Diniz, 2014)

- Filtering and preprocessing different signals before analysis.
- Analyzing and discovering different patterns in a signal.
- Visualizing and measuring different timing and frequency related characteristics of a signal.

5 Hardware Implementation

5.1 Process Flow

The major step in the hardware implementation of a signal processing algorithm is VHDL coding. The process flowchart is shown in Fig. 7 (Li et al., 2020).

In Fig. 7, the following steps are there in the whole process (Apolinário & Diniz, 2014):

- Start with a top-level block diagram describing major blocks, inputs, and outputs
- Determine approximate latency and output (throughput) of each block in the diagram. Throughput is determined by the clock speed and data width. Latency is defined by the number of pipeline stages.
- Think about the micro-implementation of each block in terms of state machines, RAMs, ROMs, and datapath.
- Prototype the hardest and least clear parts of the algorithm. This step will ensure that it is feasible to implement the algorithm; there is enough area on the chip/FPGA, and performance goals can be met.
- Implement the rest of the algorithm.

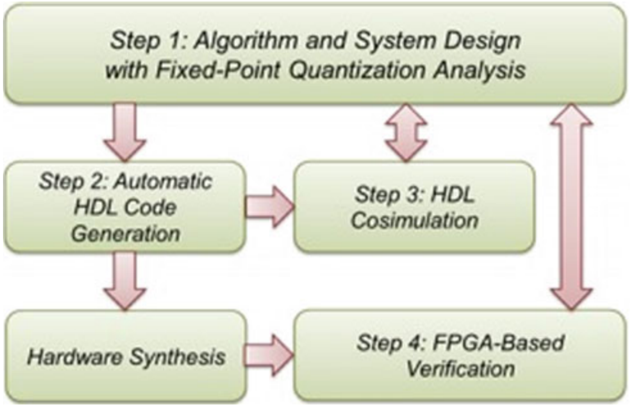


Fig. 7 Process flow of hardware implementation of an algorithm

- Synthesize and place and route the design.
- Develop test cases and simulate the design.
- Iterate between routing design and test case development until all simulation test cases are passed, and design meets area and performance goals.

5.2 Languages Used

The basic part of hardware implementation is done with the coding that requires a language for defining its structural and behavioral statements and defining operations related to both software and hardware. There exist many languages that were developed to assign hardware description. Some of them are still in use while others have become obsolete due to their flaws and limited library design. The design languages are divided into two categories: software programming language (SPL) and hardware description language (HDL).

HDLs belong to a vast field that needs exhaustive exploration since they contain multiple nested loops of instructions making them hard to debug even by professional programmers. There can be for-loops and switches along with non-blocking statements and wires that use to behave and appear beyond imagination in comparison to the conventional languages.

VHDL (Grout, 2008) and Verilog platforms are the most famous and preferred out of all HDLs. Most of the CAD tools, nowadays, support these languages. These are also endorsed and are included in IEEE standards. Other types of HDLs can be Java-HDL and Active-HDL (Grout, 2008).

In the early 80s, fast changes and advancements in design technology needed to develop standard design practices. In 1983, VHDL was developed by US Defense, under the very high-speed integrated circuits (VHSIC) program (Grout, 2008). It was then used to define complex circuits and their behavior which are then fed to the software programs to simulate any circuit's operations. Due to its versatility, IEEE adopted it as standard 1076 (VHDL-87), in 1987. It was revised to VHDL-93 in 1993.

5.3 Hardware Used

The process for hardware implementation of signal processing algorithms using ASICs or FPGAs is described next.

5.3.1 Application-Specific ICs (ASICs)

In daily life, different gadgets used are usually developed based on integrated circuits (IC) technology. This technology has reduced the size of an IC by increasing the density of components per unit area (packing density) (Grout, 2008). Generally, various ICs are specific to an application, or sometimes it is reprogrammable for different applications.

ASICs are specific ICs, where the circuits are application-specific or customized for any specific application. For example, ICs used in toys, interfacing memories to microcontrollers, etc., are ASICs. These ICs are designed for a single application and behave accordingly (Harris & Harris, 2016).

An advantage of these ICs is that they have reduced chip size with huge functional circuits embedded in them. These types of ICs are also known as system on chip (SoC) as the whole chip will be defined as a system according to the specified application for which the IC has been designed.

Figure 8 depicts different types of ASICs, hierarchically, as

- **Full Custom**—These types of ASIC circuits are defined with logic circuits having a particular application and the programmer is not allowed to change the design at the time of programming (Harris & Harris, 2016).
- **Semi-Custom**—These types of ASIC circuits are defined with logic circuits designed with the standard libraries. The designing and customization process makes changes to the ASICs to define two types of ASICs namely, standard cell-based and gate array-based. In Fig. 9, a semi-custom ASIC block (Harris & Harris, 2016) is defined with a glimpse of array structure and the embedded block where the circuits are customized as per the requirements.
- **Programmable Logic Devices (PLDs)**—This type of ICs has standard blocks for programming purposes. The programmer programs PLD (Grout, 2008) to design and optimize different parts of the applications for which the IC is designed. The programmable microcells are programmed with the help of programmable interconnects that defines the connections between different blocks, Fig. 10 defines the position of these microcells and the programmable interconnect.
- **Field programmable logic array (FPGA)**—The FPGAs have gate array arrangements for programming where both basic logic cells and interconnects are programmable. The program configures cells and their interconnections to design any application. Figure 11 shows this arrangement and structure of a standard FPGA block (Setiawan & Adiono, 2018).

5.3.2 ASIC Design Flow

The stepwise process and design dataflow for ASIC are defined as shown in Fig. 12 (Setiawan & Adiono, 2018).

Figure 12 shows the stepwise process of ASIC design dataflow described as (Rodrigues et al., 2005):

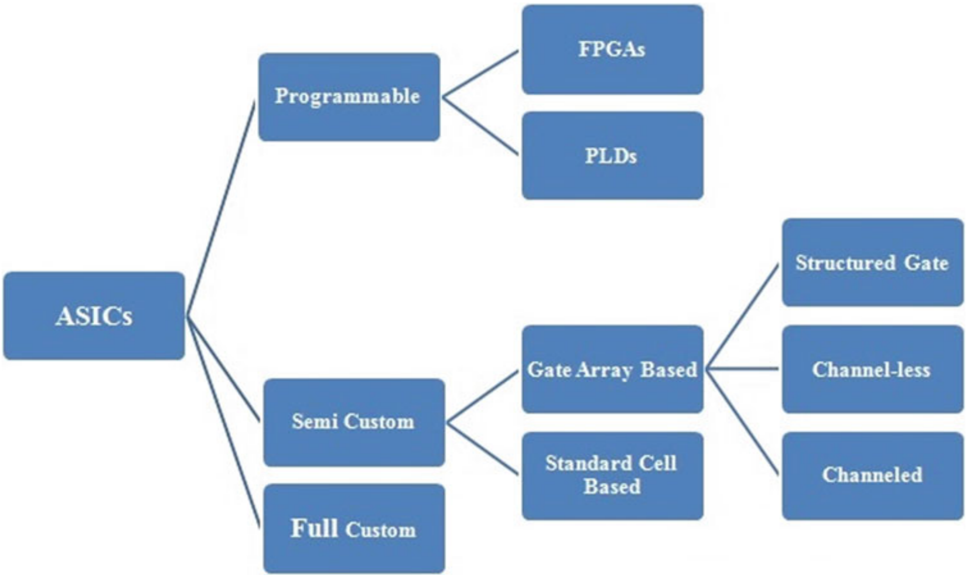
- **Design Entry**—The design of any circuit is implemented with the hardware description languages.
- **Logic Synthesis**—The interconnections and cells for the circuit are prepared according to the behavior of the circuit.
- **System Partitioning**—The size of the circuit is conditioned for ASIC size.
- **Pre-Layout Simulation**—Simulation testing is done to identify errors in the circuits.
- **Floor Planning**—The process of designing different blocks and their arrangement for any application over the ASICs.
- **Placement**—Different locations for the circuits of any single block will be decided and designed.
- **Routing**—The process to design the interconnections of different cells is done.
- **Post-Layout Simulation**—This process is done to make the layout design before the manufacturing of ICs to check the system functions and their simulations (Rodrigues et al., 2005).

Till now the discussion pertained to the ASICs and FPGAs as hardware platforms for the implementation of signal processing algorithms. A new perspective is introduced in the next topic for the hardware implementations over graphics processing units (GPUs). Here, different aspects and specifications of GPUs are discussed to replace ASICs and FPGAs (Onat, 2018).

6 Heterogeneous Computing Platforms

The use of different platforms for algorithm implementations must be identified and specified. In this section, the characteristics and features of the hardware required for the algorithm implementations will be discussed.

Fig. 8 Types of ASICs



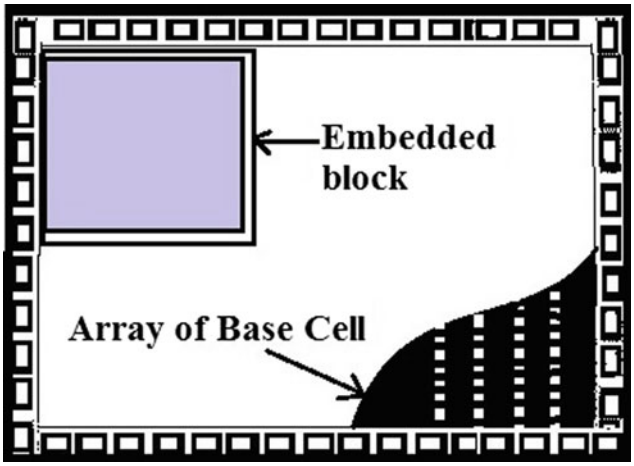


Fig. 9 An ASIC block

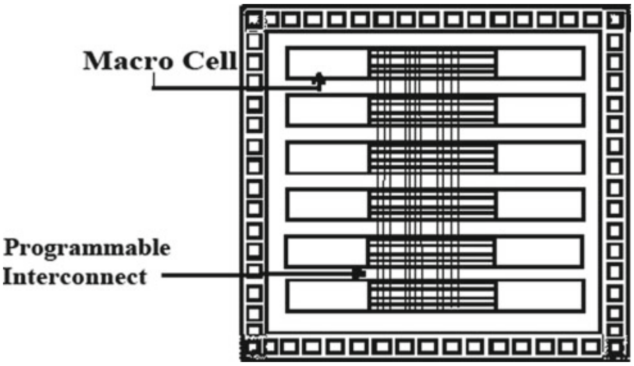


Fig. 10 A PLD block

The heterogeneous computing for any system is known as the quality of having more than one type of core or processor defined for increasing the performance or efficiency of the system. These cores or processors attain special processing qualities for the specified functions having an evolutionary design path for high-performance computing. These can achieve good performance by using parallel processes in place of enhancing clock frequencies (Andrade & Crnkovic, 2018).

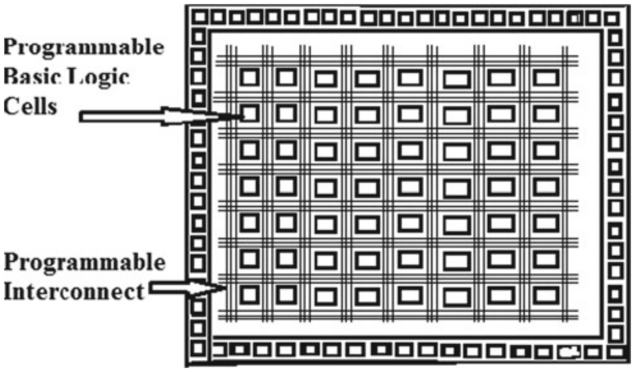


Fig. 11 An FPGA block

In the next section, different heterogeneous computing platforms are summarized.

6.1 Multi-core Architectures

They intend to use a high level of parallelism and co-processing architectures to deliver approximately 3–4 times more performance per watt. This is defined for the 3D image reconstruction in computed tomography (king of scanning) and it was initialized through FPGAs. Figure 13 shows the architecture of a single multi-core processor (https://www.arrow.com/).

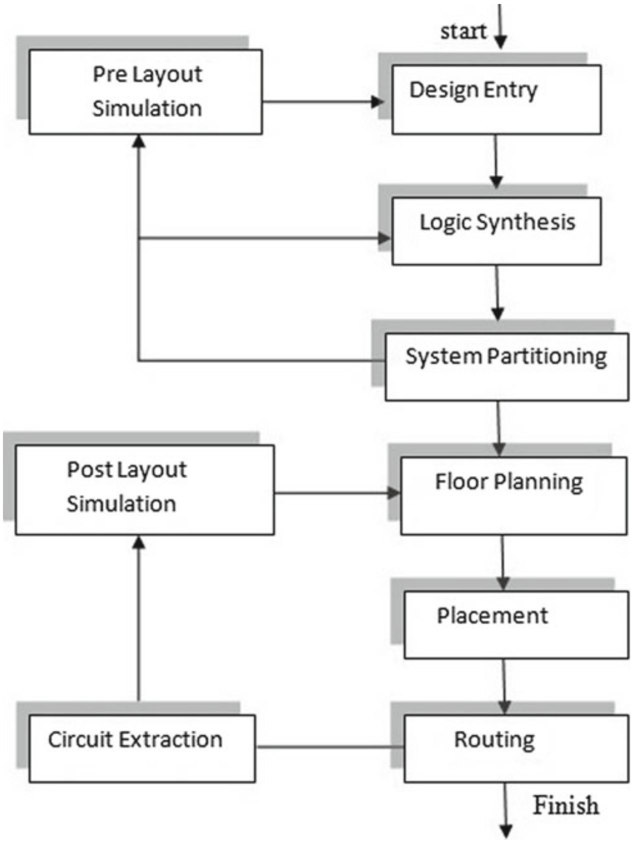


Fig. 12 ASIC design flow

6.2 DSP/CPU Processor Architecture

Keystone II multi-core processors comprising a quad-ARM Cortex-A15 MP Core processor with up to eight high-performance DSPs using the Keystone II multi-core architecture. This was applied to a cloud radio access network (RAN) station. The DSP processor architecture (https://www.arrow.com/) is shown in Fig. 14.

6.3 System on Chip (SoC)

FPGAs have evolved by including processors on them. These are effective and combined hardware and software systems where FPGA's programmable feature is used to accelerate the data-intensive computation (https://www.arrow.com/), and the associated processor is used for control and interfacing. Figure 15 shows a single SoC cell architecture depicting all the blocks and their workflow directions (Setiawan & Adiono, 2018).

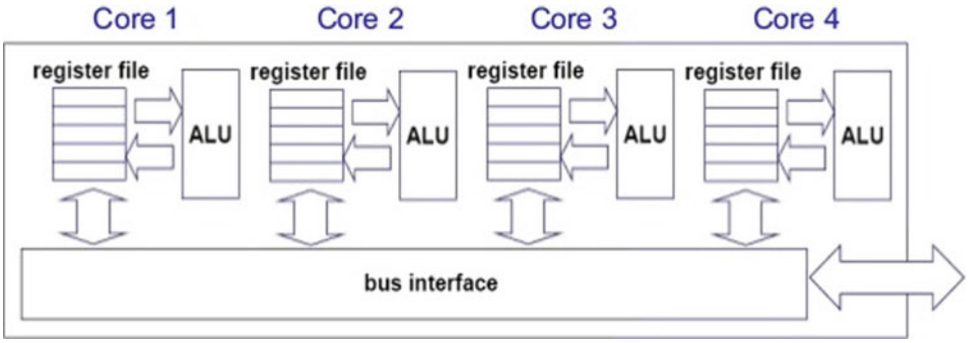
7 Graphical Processing Units (GPUs)

7.1 Accelerators

It is an add-on hardware or software program that enhances the performance of a system (Cardoso et al., 2017). There are different types of accelerators summarized as,

- **Accelerator for hardware**:
  It is used to enhance the run time and performance characteristics (Cardoso et al., 2017) of the system by performing functions faster than the central processing unit (CPU).
- **Accelerator for graphics**:
  It enhances the graphics rendering capability.
- **Accelerator for cryptography**:
  It helps in faster encryption and decryption processes.
- **Accelerator for Web**:
  It works as a proxy server that improves and enhances the speed of the internet.
- **Accelerator for PHP**:
  It speeds up the PHP applications for computing purposes.

Fig. 13 Single multi-core architecture



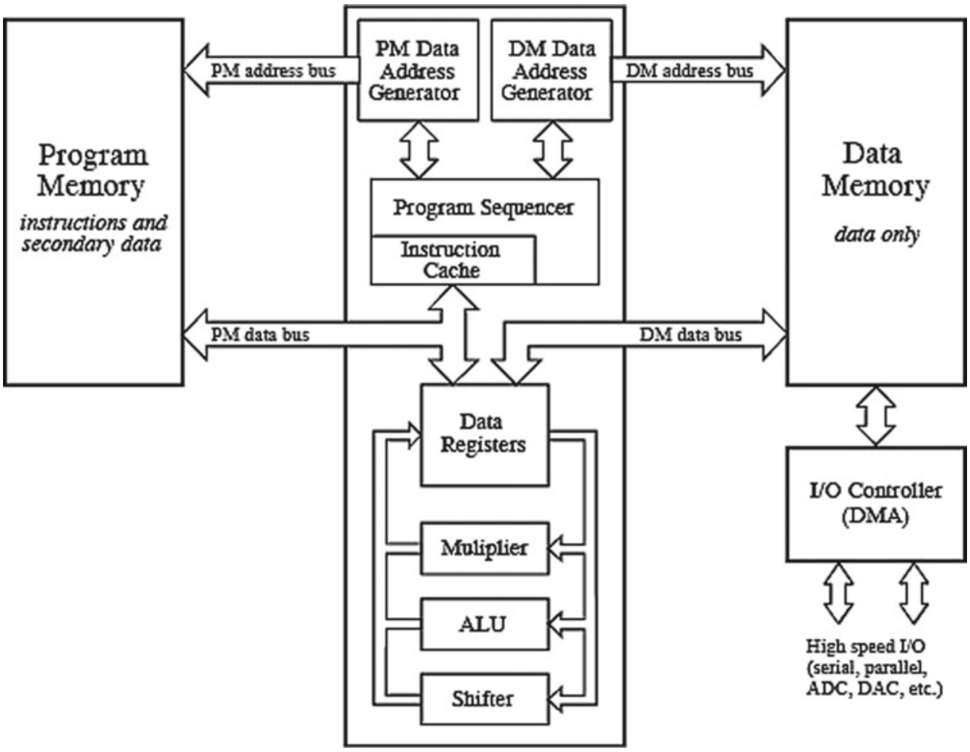


Fig. 14 DSP/CPU processor architecture

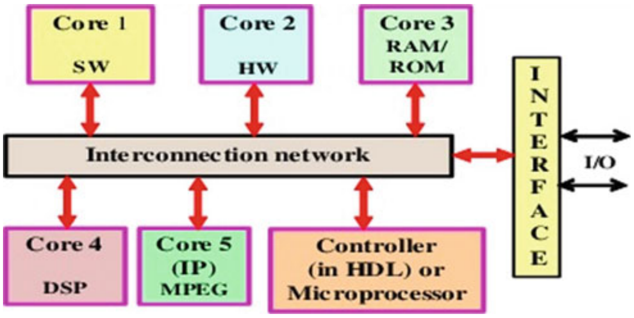


Fig. 15 SoC architecture

7.2 GPU-Accelerated Computing

This type of computing is implemented using a GPU along with a CPU to enhance process-intensive functions like deep learning, analytics, and engineering applications. It is popular due to its huge variety of applications such as artificial intelligence, robotics, or automated smart cars (Crespo et al., 2011).

The GPU provides better performance for software applications and makes them faster. GPU-accelerated computing is processed by enhancing its computation-intensive parts by the GPU while other sections are being executed in the CPU (Srivastava & Pandey, 2013). A CPU comprises cores designed for sequential serial processing while parallel architecture consists of more efficient and smaller cores that can handle multiple tasks simultaneously. As a result, sequential calculations are performed in the central processing unit while highly complicated calculations are computed in a GPU at the same time in parallel. It is another salient feature to support all the parallel programming models helping the application designers and developers to ensure superior application performance (https://www.bertendsp.com/). This type of accelerated computing has been rigorously used in various processes such as video editing, medical imaging, fluid dynamics simulations, color grading, and enterprise-level applications. Also, it has been effectively used in complex fields (Crespo et al., 2011) such as artificial intelligence and deep learning.

7.3 The Architecture of GPUs

To understand the functions and operations of GPUs, their architecture perspectives presented to understand different parts and functions. Any ASIC or CPU is defined to handle different tasks like time slicing, machine emulation, branching, security, complex workflow, etc., whereas a GPU can execute repetitive low-level functions (Sundfeld et al., 2020).

Traditionally, a GPU has thousands to lakhs of arithmetic logic units (ALUs) compared to the traditional ASIC or CPU which has approximately 4 to 8 ALUs as shown in

Fig. 16 which is a diagrammatical structural comparison between a GPU cell and an FPGA (CPU) cell (https://www.bertendsp.com/). The comparison of the floating-point functioning capability between CPU and GPU is that it later is highly specified for the parallel computation of intensive functions and applications. They are, therefore, designed with more transistors devoted to data processing in place of data caching and workflow control applications (Srivastava & Pandey, 2013).

GPUs are used for handling applications involving large data values using data-parallel models to realize faster computations. Many algorithms are accelerated using data-parallel processing that ranges from signal processing to complex computational finance or biology processing (Mohanty, 2009).

The arrival of multi-core GPUs changed the usual processor chip structure into parallel systems. The challenge is to develop application software that transparently scales parallel processes to increase processor core functions, like 3D graphics applications for scaling their parallelism to multi-core GPUs with huge numbers of cores (Mohanty, 2009).

7.4 Programming GPUs

The coding language must be structured and defined so that the programs should control the data flow for different processes and operations for a GPU. On their first use, the codes must be mapped on the matrix operations for the functions of different parts, which is a difficult task and requires a lot of time and dedication. But nowadays, high-level languages like CUDA, OpenCL, or OpenACC target the GPUs directly and results in bringing GPU programming into the mainstream (Shi et al., 2018).

A GPU program includes two parts, viz.

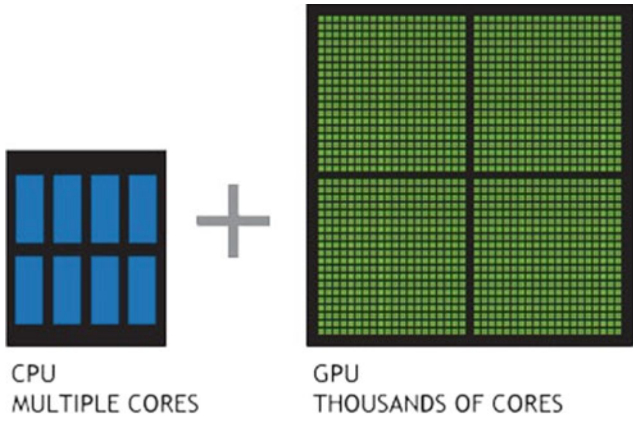


Fig. 16 Structure of CPU and GPU

- The first part is the host part which runs on a CPU with one or more kernels used to set up parameters and select data for the computations.
- The second part is the kernel part which performs the computations.

7.5 Hardware Requirements for GPU Programming

Modern GPUs are like computers physically even though they serve a bigger computer system. They relate to the host by using a high-speed I/O bus slot, viz. Peripheral Component Interconnect-Express (PCI-E). They are high energy-consuming as some of them can consume hundreds of watts of power or sometimes higher due to their complex structures and involvement of more sophisticated processes as compared to those handled by other parts of the computer system. Therefore, they need to dedicate their memory, control chip along with many processors or ALUs (Srivastava & Pandey, 2013).

Nowadays, GPUs contain a few gigabytes of onboard memory. For instance, NVIDIA's GeForce series and ATI/AMD's Radeon series (Safari and Mekhilef, 2011) have a hundred megabytes to gigabytes onboard memories. Professional GPUs are defined for high-definition image processing and complex computations. The data transferred between onboard memory and host memory is done by direct memory access (DMA) process, so the language must be designed to support DMA between the host and onboard memory. The GPU executes computationally intensive processes while onboard memory supports a high data bandwidth.

The GPUs have many processors that are known as streaming processors (SP) which can process a sequential thread. They have "Fermi architecture" comprising streaming multiprocessor (SM) which includes 32 streaming processors. It can have one or more multiprocessors onboard. Along with the streaming processors, each of them is also equipped with two warp schedulers, two special function units (SFUs), a set of 32-bit registers, and a configurable shared memory of 64 KB size. A warp scheduler processes thread control, SFUs controls transcendental and double-precision operations. For a "Kepler architecture," the 192 streaming processor is included with a single multiprocessor. It has more warp scheduler and built-in SFUs.

The software configures a small data cache named shared memory or L1 cache and the same is shared among all the streaming processors within one multiprocessor. The shared memory has low latency (processing speed) and high bandwidth compared to the onboard memory. A single multiprocessor has 64 KB of shared memory and is configured by special commands. Shared memory is distributed between software and hardware data cache. The user can choose to assign 48 KB to software and 16 KB to the hardware data cache. The architecture for the parallel threading of a GPU is shown in Fig. 17 (Srivastava & Pandey, 2013).

7.6 Languages Required for GPU Programming

GPU identifies the computational problems with the help of graphics primitives where earlier efforts are made to use GPUs as general-purpose processors that are required to reformulate computational problems in the language of coding (Siddappa & Wickert, 2019). In modern times, coding platforms ignore language barriers and focus on high-level computing. There are some prominent and famous coding languages to fulfill all these requirements and conditions are (Sehgal et al., 2020):

- **Compute Unified Device Architecture (CUDA)**
  This platform was released by NVIDIA in 2007. It can speed up the computing processes by the best use of GPU power. The programmers can call or fetch CUDA from other languages also like C, C++, Fortran, or Python without having good skills in graphics programming. The CUDA-toolkit includes the start-up kit needed by a programmer to start to create GPU-accelerated applications that perform the CPU-bound counterparts. The CUDA-SDK is defined for Windows, LINUX, and MAC-OS. The CUDA platform also supports different computational interfaces like OpenCL, Direct Compute, OpenGL Compute Shaders, and C++ AMP.
- **Open Computing Language (OpenCL)**
  This platform was released by the Khronos Group in 2009. It is a popular open source and free standard of cross-platform parallel programming. It improves the speed and response timing of many applications like vision processing, neural network, professional creative tools, and scientific and medical software. Until now, it is implemented by AMD, Apple, IBM, Intel, NVIDIA, Samsung, Vivante, Altera, Xilinx, and Ziilabs and supports approximately all popular operating systems for all major platforms that make it very versatile. It is defined as a C like language for writing programs, but third-party application program interfaces (APIs) need to be defined for other programming languages like Python or Java also.
- **Open Accelerators (OpenACC)**
  It is the newest standard for parallel computing and was released by a group of companies like Cray, CAPS, NVIDIA, and the Portland Group, in 2015, to simplify parallel programming of different heterogeneous GPU systems. It is a programmer-driven, directive-based, performance-portable parallel computing model designed to port the codes of different varieties of heterogeneous

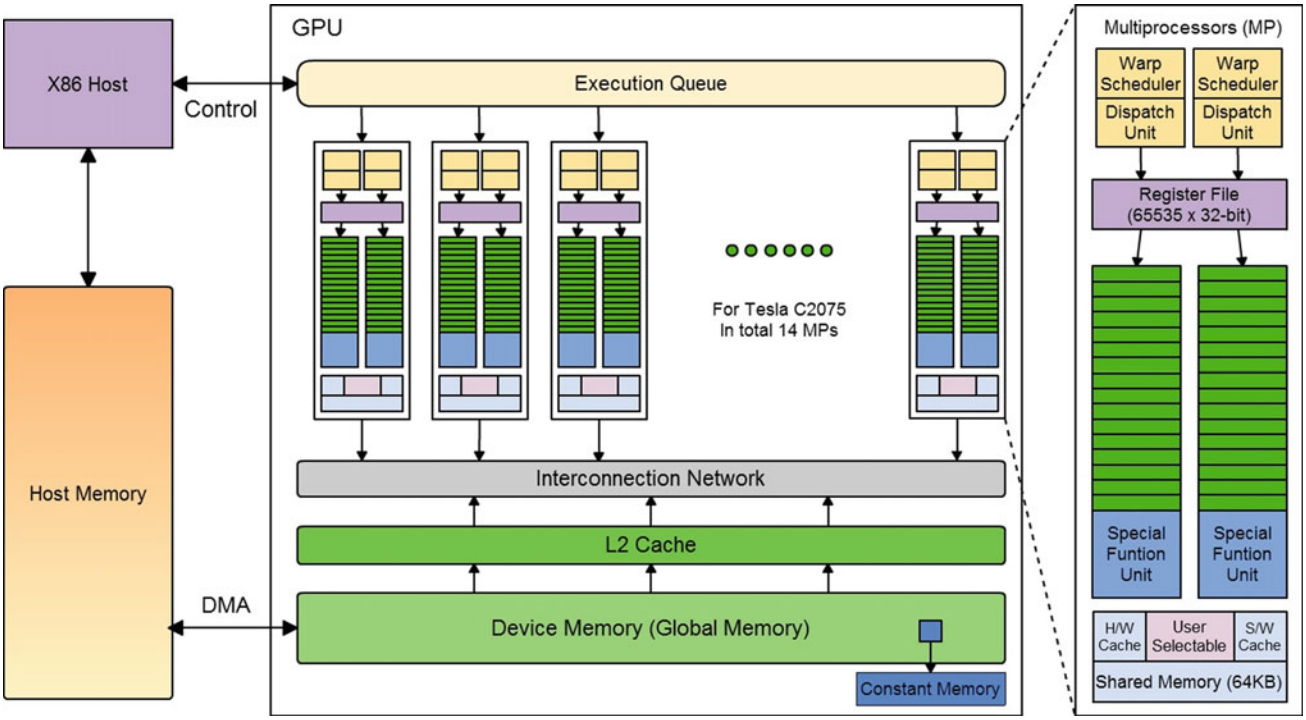


Fig. 17 Data-parallel threading model of a GPU

high-performance compute (HPC) hardware architectures with the least effort. It can define C, C ++, and Fortran source code to dedicate the GPU for the portions that should be accelerated. The goal for OpenACC is to define a model for accelerator programming which is portable across various OS and various host GPUs and accelerators.

8 Comparison of GPUs, FPGAs, and ASICs

This section is focused on a comparative study of the hardware platforms available for the implementations. For resources demanding signal processing algorithm implementations, the chosen hardware platform should have an edge over others for the purpose (Apolinário & Diniz, 2014). In the previous sections, aspects involving the structural, behavioral, and programming of different hardware platforms have been discussed. Therefore, a comparison of different platforms based on some important factors and specifications is presented next to help in deciding the preference and priority of a hardware platform.

- **Architecture**
  The ASICs contain IC-level circuits that are optimized for end applications whereas FPGAs have a flexible collection of logic blocks that can be programmed and altered. On the contrary, GPUs are designed to be used in a huge range of intensive computational applications.
- **Processing**
  The ASICs and FPGAs are only designed for application-specific processing, but the GPUs are designed with thousands to lakhs of processor cores for a variety of applications.
- **Programming**
  As per the programming aspect, ASICs are application-specific, and the manufacturers define new tools with the new ASIC ICs. The FPGAs are programmed traditionally using HDL (Verilog and VHDL) coding languages except for some programmed using C or C++. For signal processing algorithms, one needs to simulate the algorithms on MATLAB first, then only the algorithms can be realized on ASICs or FPGAs. But in the case of GPUs, this constraint of the need for two different languages has been solved by programming languages for GPUs like CUDA, OpenCL, Python, or OpenACC, which are capable of both simulation and implementation. Another advantage of these languages is that they are open source, i.e., can be used by any user free of cost.
- **Peripherals**
  The peripherals included in ASICs can be USB, Ethernet, or any industry-standard functions due to their application-specific functionality whereas FPGAs include different transceiver devices and configurable I/O banks. The GPUs provide the benefit of having the least number of peripherals to be connected as it requires only cache memory.
- **Applications**
  The ASICs have the applications specifically defined with the optimum combination of performance and power consumption whereas the FPGAs have specific applications with the benefit of reconfiguration of the chips with parallel processing. On the contrary, GPUs have the massive processing power for applications such as video processing, image processing, or signal processing.

Because of the above discussion, cutting-edge benefits based on different physical and technical parameters of GPUs (Andrade & Crnkovic, 2018) have been identified in comparison to those provided by ASICs and FPGAs. There is an important benefit of the requirement of the minimum hardware and the availability of open-source programming languages (Apolinário & Diniz, 2014). Therefore, GPUs would be a better choice for hardware implementations of signal processing algorithms. Different comparison parameters and their effects on the applications are shown in Fig. 18, which depicts a graphical presentation of comparison between FPGA and GPU.

9 Conclusion

A wide variety of facts have been presented and discussed to establish the superiority of GPU for signal processing algorithm execution and implementation successfully. This is due to their cutting-edge design of parallel processing framework involving a huge number of complex computing units in the architecture, unlike limited numbers as used in

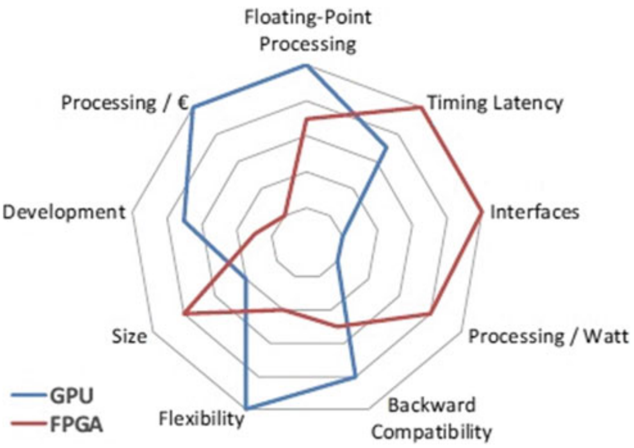


Fig. 18 Qualitative comparison of GPU and FPGA

ASICs or FPGAs. This complex architecture of the GPU is well suited for signal processing, video processing, or image processing applications.

There is another aspect of the cost of any system designed over GPUs, and it requires minimum peripherals compared to FPGA or ASIC and requires a single coding language for both the simulation as well as implementation processes which is, in many cases, an open-source language which is easily and freely available for the user, whereas, ASIC or FPGA requires two different languages, one for simulation (MATLAB Tools) and other for the hardware implementations which are typically licensed programming language for the particular ASIC or FPGA ICs.

This benefit makes a great impact on using GPU stand-alone systems over ASICs or FPGAs.

GPUs are the best-chosen platform for hardware implementations due to some of the general features which enhance the functionality and performance of the implemented system compared to FPGA platforms, like faster processing, floating-point processing, flexibility in implementations, reduced costing, as discussed previously. These benefits lead GPU to have some of the best applications like graphics processing, computer vision, bioinformatics, computational finance, data intelligence, machine learning, big data processing, and weather: fluid dynamics.

So, in every aspect of the technical, physical, and behavioral specifications, the GPUs can be the best choice for the signal processing algorithm implementations which will be cost-efficient also. The GPU system can also be used as a single device or stand-alone system for all types of signal processing algorithm implementations, as the system is reconfigurable and robust for programming, as well, and would be the best choice for the applications related to signal to process.

References

Andrade, H., & Crnkovic, I. (2018). A review on software architectures for heterogeneous platforms. In *2018 25th Asia-Pacific Software Engineering Conference (APSEC)*, Nara, Japan, pp. 209–218.

Apolinário, I. F., & Diniz, P. S. R. (2014). Academic Press Library in Signal Processing. Program of Electrical Engineering and the Department of Electronics and Computer Engineering, COPPE/Poli, Universidade Federal do Rio de Janeiro, Brazil, Vol. 1, pp. 3–28.

Arrow Electronics guides. https://www.arrow.com/.

Berten Digital Signal Processing, White Paper. https://www.bertendsp.com/.

Cardoso, J. M. P., Coutinho, J. G. F., & Diniz, P. C. (2017). *Embedded Computing for High Performance*. Morgan Kaufmann.

Crespo, A. C., Dominguez, J. M., Barreiro, A., Gómez-Gesteira, M., & Rogers, B. D. (2011). GPUs, a new tool of acceleration in CFD: Efficiency and reliability on smoothed particle hydrodynamics methods. *Journal of PLOS ONE, 6*(6).

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Grout, I. (2008). *Digital Systems Design with FPGAs and CPLDs*. Newnes Publication, pp. 177–216.

Han, M., Song, J. M., Yang, H. G., & Kim, Y. (2018). Implementation of multi-channel FM repeater using digital signal processing algorithm in FPGA. In *International SoC Design Conference (ISOCC)*.

Harris, S. L., & Harris, D. M. (2016). Digital design and computer architecture. *ARM Edition*, 172–237.

Kiran, M., War, K. M., Kuan, L. M., Meng, L. K., & Kin, L. W. (2008). Implementing image processing algorithms using 'Hardware in the loop' approach for Xilinx FPGA. In *2008 International Conference on Electronic Design*, Penang, pp. 1–6.

Li, G., Chang, Q., Xi, C., & Ma, X. (2020). Acquisition design and implement of Beidou B3I signal based on GPU. In *IOP Conference Series: Materials Science and Engineering.* (Vol. 715, no. 1).

Mohanty, S. P. (2009) GPU-CPU multi-core for real-time signal processing. In *2009 Digest of Technical Papers International Conference on Consumer Electronics*, Las Vegas, NV, pp. 1–2.

Onat, E. (2018). FPGA implementation of target detection algorithm at real-time video signal processing using harris corner detector filter. In *26th Signal Processing and Communications Applications Conference (SIU)*.

Raut, N., & Gokhale, A. (2013). FPGA implementation for image processing algorithms using xilinx system generator. *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*.

Rissa, E., Uusikartano, R., & Niittylahti, J. (2002). Adaptive FIR filter architectures for run-time reconfigurable FPGAs. In *Proceedings, IEEE International Conference on Field-Programmable Technology*.

Rodrigues, J., Kamuf, M., Hedberg, H., & Owall, V. (2005). A manual on ASIC front to back end design flow. 75–76.

Safari, A., & Mekhilef, S. (2011). Simulation and hardware implementation of incremental conductance MPPT with direct control method using Cuk converter. *IEEE Transactions on Industrial Electronics, 58*(4), 1154–1161.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IoT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Setiawan, E., & Adiono, T. (2018). Implementation of systolic co-processor for deep neural network inference based on SoC. In *International SoC Design Conference (ISOCC)*.

Shi, L., Gao, X., Yang, X., Chen, Z., & Zheng, M. (2018). Algorithm optimization and hardware implementation for merge mode in HEVC. *Journal of Real-Time Image Processing*.

Siddappa, C., & Wickert, M. (2019). CAF implementation on FPGA using python tools. In *Proceedings of the 18th Python in Science Conference (SCIPY 2019)*.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of Things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth, 2,* 191.

Srivastava, J. B., & Pandey, R. K. (2013, June). Implementation of digital signal processing algorithm in general purpose graphics processing Unit (GPGPU). *International Journal of Innovative Research in Computer and Communication Engineering 1*(4).

Sundfeld, D., Teodoro, G., Gorodkin, J., Melo, A. C. M. (2020). Using GPU to accelerate the pairwise structural RNA alignment with base-pair probabilities. *Special Issue in Parallel, Distributed, and Network-Based Processing*.

Woods, R., & Yi, Y. (2017). *FPGA Based Implementations of Signal Processing Systems*. Wiley.

The Role of IoT and Narrow Band (NB)-IoT for Several Use Cases

Korhan Cengiz, Basak Ozyurt, Krishna Kant Singh, Rohit Sharma,
Tuna Topac, and Jyotir Moy Chatterjee

Abstract

Internet of things (IoT) and its improved version narrow band Internet of things (NB-IoT) use smart networks to meet the needs of the modern world. These components are very important for collecting data from the environment and correctly managing the related scenarios, and thus more use of wireless networks in IoT-supported heterogeneous networks. Decision making is the main component in the IoT universe, and this function's consistency depends on the accuracy of the data obtained from the sensor nodes. IoT and NB-IoT are the most exciting cutting-edge technologies for solving above-mentioned problems. IoT supports many revolutionary commercial and social solutions, including food production, wearable or inconspicuous medical sensors, Industry 4.0, power, water grids, smart cities, education, transportation and road infrastructure needs. Industry 4.0 symbolizes the beginning of the Fourth Industrial Revolution. Industry 4.0 represents the current trend of automation technologies in the manufacturing industry and primarily covers cyber-physical systems (CPS), IoT and cloud computing at the moment, low power wide area network (LPWAN) is a promissory and highly effective solution for IoT and machine-to-machine (M2M) communication-based applications with long range and low power consumption. With the eagerly awaited developments in artificial intelligence, machine learning, data analysis, and block chain technologies, LPWAN applications have the potential to undergo epic expansion in nearly every area of society, business, and industry. This chapter aims to stimulate a discussion about the role of IoT and NB-IoT which can play in overcoming the limitations of a wide-ranging deployment of autonomous networks and their usage in real-world phenomena.

Keywords

IoT • NB-IoT • Industry 4.0 • LPWAN • Cloud computing • IoE

1 Introduction

IoT technologies have evolved in the last decades, and they have been used in numerous areas. Because almost all things are connected by this network today,. the IoT acquits itself well as contributing to data processing, efficiency, and heterogeneity. Of late, IoT communication technologies have reached a higher level of maturity and prevalence due to the development of IoT. Based on touch distance, new era communication can be classified by the following categories: limited with short coverage and unlimited ones. The former ones are represented short-distance communication technologies. They are typically used in the smart home. The platform is desirable for services with low data charges such

---

K. Cengiz (✉)
Department of Electrical-Electronics Engineering, Trakya University, Edirne, Turkey
e-mail: korhancengiz@trakya.edu.tr

B. Ozyurt
Faculty of Applied Sciences, Trakya University, Edirne, Turkey
e-mail: basakozyurt1@trakya.edu.tr

K. K. Singh
Department of Computer Science & Engineering,Faculty of Engineering & Technology, Jain (Deemed-to-be University), Bengaluru, India
e-mail: krishnaiitr2011@gmail.com

R. Sharma
SRM Institute of Science and Technology, Chennai, India
e-mail: rohitapece@gmail.com

T. Topac
Institute of Computational Sciences, Trakya University, Edirne, Turkey
e-mail: tunatopac@gmail.com

J. M. Chatterjee
Lord Buddha Education Foundation, Kathmandu, Nepal
e-mail: jyotirchatterjee@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_11

as intelligent parking, that industry defines as low power wide area network (LPWAN). This chapter describes some use cases of one of LPWAN technologies has been particularly self-explanatory. Cellular mobile communication has long been mainly assisted the people-prompting services for voice and the broadband services of mobile technology. The narrowband Internet of things (NB-IoT) is a low power wide area massive one that propounded by 3GPP for data sensing and gathering and is used for intelligent applications with low data rates. Common examples of applications are environment monitoring and meter systems. The NB-IoT provides solid connectivity, wide area coverage, two-way tripping between signaling level and data level, and it consumes too little power. This technology is also assisted by networks that use cellular systems. NB-IoT use cases can be categorized as public and personal. This chapter focuses on public use cases. As world population grows up, people interact with each other frequently and basic needs have to be issued. For example, health care is the most vital an expensive one for governments and it can grow apace. To handle this situation, the system has to put in time. It is an unmentionable economic pressure for governments. Seeing as saving time and money, the technology is a must. In twenty-first century, the IoT is the frontrunner for the conjuncture. NB-IoT is the one that shines out most. It assists to the core of social life and industry. That is why, we entitle industry and cities as smart ones. Apart from urban life, NB-IoT concurrently interferes agriculture in a good way. Indeed, the industry has been the sum of agriculture for millenniums. Over the past decade, it has channeled the Gaia. This situation has been rush-hour for last decade. The Industry 4.0 steers the economy in all its parts. For certain, the industry activity on Earth has consequences. These are garbage guidance and pollution profiling problem. Humankind has to look in face of both. Otherwise, our learning outcome will get into danger in a short span of time. If we live in union, we have to respect each other's right. In daily life, parking is an ordinary need for drivers and disburdens the traffic. In order to conduct routine doing in urban, the parking problem should be hurdled. The NB-IoT comes to driver's aid for parking challenge. This greatly serviceable here at, any accident can be prevented. The citadels of industry are factories. To cope with economic downs, these citadels must work properly. They ought to have self-management on behalf of rapid turn out progress. The NB-IoT has become a part of self-management for recently. World has waters and lands as all know. We can populate on lands easily, but we also need waters to live. To fulfill this human aspiration, NB-IoT helps us above or below sea level. So, recently NB-IoT for maritime that uses has been applied on waters. Improvements of the IoT become prominent, too. Thus, it has potential to get to the top of technology in a very short time. This book chapter is organized as follows: Section 2 highlights NB-IoT Physical Features. Section 3 elaborates varied use cases of Real-World NB-IoT. Section 4 concludes the chapter with future scope.

2 NB-IoT Physical Features

Long standby times can be obtained with the power-saving mode (PSM) and extended discontinuous reception (eDRX) at this technology. In network that uses NB-IoT, end device's lifespan in terms of battery should be 10 years and use low-frequency rate typically (Chen et al., 2017).

In accordance with the TR45.820 simulated data, it could be affirmed that in independent deployment mode NB-IoT can arrive at 164 dB in terms of deck power. Presently, the acceptable level in terms of latency is 10 s in 3GPP IoT. Indeed, lower latency time is 6 s for the highest coupling losses. This can be achieved as well be supported (Chen et al., 2017).

The NB-IoT which is an essential LTE furtherance has typical narrow band characteristics. RF channel capacity on physical layer of NB-IoT is 200 kHz. On the other hand, the protocol of the NB-IoT high layer is controlled by minor revisions of some LTE. Power consumption level and multi-connection and used less data (Chen et al., 2017).

Its IoT is the core service to appeal to a larger user group on the market for communications services in the future. In China, the four most profound telecom operators have worked on NB-IoT by the way of spectrum resource. That is strongly braced by China industry. In response, a commercial network has been established by China Unicom for NB-IoT.

NB-IoT supports three following types of deployment scenarios, and they have 180 kHz BW:

- *Independent* provides a bandwidth that does not duplicate the LTE's.
- *Guard band* uses the side frequency band of LTE.
- *In-band* requires 1 PRB LTE frequency band for deployment.

There are five parts of NB-IoT network:

Terminal: If SIM card is installed on devices, all industries can enter in the process of the network usage.

Base station (BS): Telecom operator has BSs for a long time, and NB-IoT can be adopted by them.

Core network: Via this layer the base station is able to communicate with the cloud.

Cloud platform: This platform has varied functions, and outputs being delivered to the business distributions are vertical or terminal.

Vertical business center: The center can receive the data coming from service within operation center of its own and takes control of the terminal.

NB-IoT users usually transfer mini packages so with NB-IoT, making longwinded display of channel quality variations is difficult; therefore, it performs a scope ratio rather than a mobile connection adjustment plan. Three types of cover classes are existed. They are normal, robust, and extreme.

The applied mechanism of NB-IoT forwards data, so it gains diversity of time and productivity in demodulation by giving less instructions in modulation and purview output. Forwarding of data is allowed by channels of all.

3 Use Cases of Real-World NB-IoT

By virtue of its forms of using, it can satisfy the aftermarket needs for low power with low data rate, long range, and massive capacitance, but it is hard to facilitate dense mobility, it is not suited for services that need much mobility, low latency, discrete motion, or real-time data transfers.

Automated exception reporting facilities: Smoke detector, smart metering note, etc.

Independent periodic reporting agencies requires communication process that has a relatively small size of uplink data and short transmission cycle like daily or hourly: Representative fields of application are measurement protocols for intelligent public services and extended tillage sector and ambient.

Command services on networks: This type of services manages to meter all transfers and logs, etc.

Software update service: This employment upgrades size of data size of data that are used while downloading or uploading daily or hourly.

Specific urban application scenarios of NB-IoT are classes of intelligent city, environmental monitoring, user-friendly tasks, and smart examination of organisms (Cole Reports, 2020). Included are intelligent portable devices, smart home, trash cans, people tracking, and such ones. Intelligent environmental monitoring includes smart farming, air or water or soil quality monitoring, and so on (Cellular IoT Market by Offering (Hardware and Software) Market Growing Trends and Technology forecast, 2020).

The NB-IoT is turning into an up and coming range of technology that has tried wireless connection to a broad count of devices used in ubiquitous surveillance of scenarios, as in Smart City, Precision Agriculture and Industry 4.0 (Cellular and Ecosystems, 2020). Figures 1 and 2 illustrate some characteristics of NB-IoT.

NB-IoT gateways between today's 2G, 3G, 4G world, and tomorrow's 5G world will probably be with us for a long time to come due to the IoT economy. Prospective fifth generation (5G) wireless systems (Cengiz & Aydemir, 2018; Aydemir & Cengiz, 2017) are deemed the most promising candidates facilitate effective cooperation between IoT devices because these devices exhibit high data rate, low latency and cost per bit, and high-frequency qualification.

3.1 Intelligent Health Care for People

The term of intelligent health care can be understood as the use of mobile and electronic technology to work up diagnosis of diseases, needers' care, and so no. Since the creation of the new network technologies as options or facilities for healthcare system, system has provided smart health care subconsciously. These networks aim to create smooth transition, user-friendly, exact and online health care for patients. If patients do not be cured with the strictest confidence and beware, the results can be fatal. LTE and 5G changed many sectors containing health system and beyond these, cloud computing followed the trend. Now, doctors are able to consult patients by using assorted sensors. If we want the healthcare institutions safer and fuss-free, we should care several factors during the sector is skyrocketing. The rocket will not have mercy for us while rising when precautions are

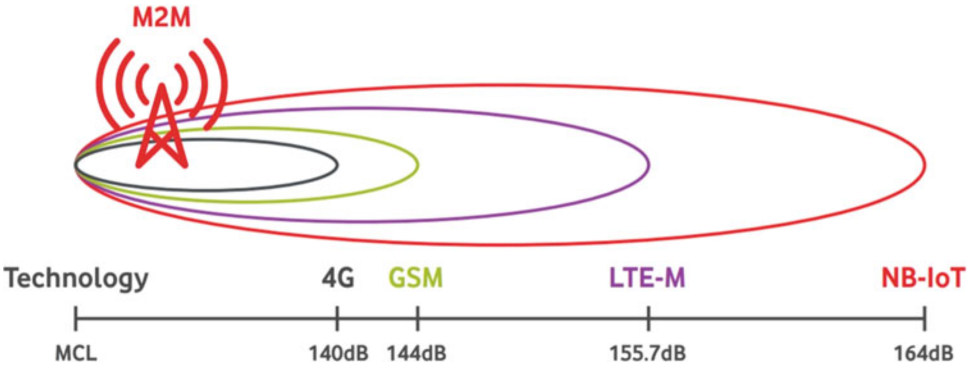
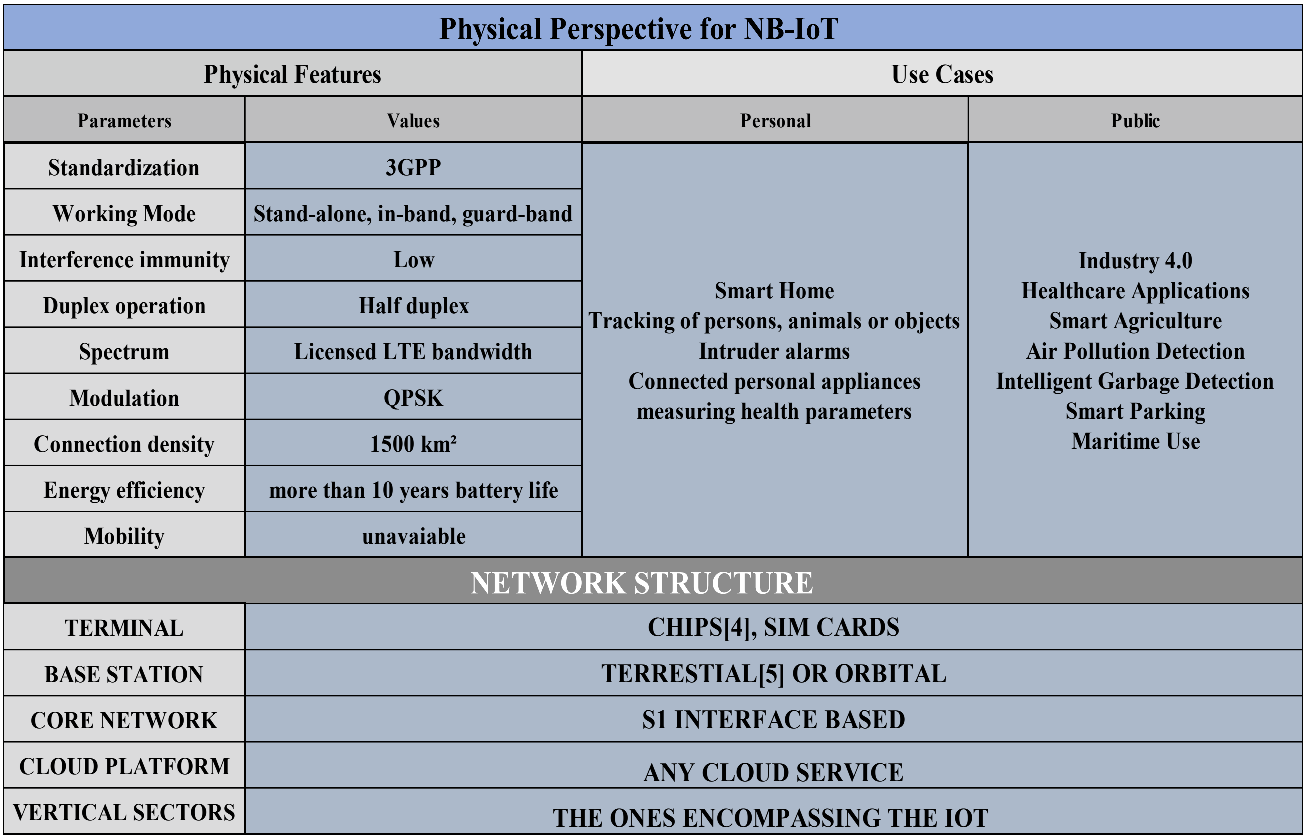


Fig. 1 NB-IoT has the capability to reach two to three double brick walls



Physical Perspective for NB-IoT

Physical Features		Use Cases	
Parameters	**Values**	**Personal**	**Public**
Standardization	3GPP	Smart Home Tracking of persons, animals or objects Intruder alarms Connected personal appliances measuring health parameters	Industry 4.0 Healthcare Applications Smart Agriculture Air Pollution Detection Intelligent Garbage Detection Smart Parking Maritime Use
Working Mode	Stand-alone, in-band, guard-band		
Interference immunity	Low		
Duplex operation	Half duplex		
Spectrum	Licensed LTE bandwidth		
Modulation	QPSK		
Connection density	1500 km^2		
Energy efficiency	more than 10 years battery life		
Mobility	unavaiable		

NETWORK STRUCTURE

TERMINAL	CHIPS[4], SIM CARDS
BASE STATION	TERRESTIAL[5] OR ORBITAL
CORE NETWORK	S1 INTERFACE BASED
CLOUD PLATFORM	ANY CLOUD SERVICE
VERTICAL SECTORS	THE ONES ENCOMPASSING THE IOT

Fig. 2 NB-IoT overall physical perspective

not taken. For that reason alone, smart doorways to information era are needed to be entrenched the quality of public health provision, notably for needers. For the sector, the monitoring should be net flow in order to that doctors can eye on patients' body functions' disorders to ensure trustworthy data. The concept in concrete terms is glorious aid for patients when emergency occurs. Most foremost quarters using related approach in the world have done durable jobs in the recent times. Meanwhile, novel approaches for system management are needed to be enlarged. Today, remote supervision methods in the healthcare sector require constant monitoring of the all parameters of the patient (Gartner sees 5.8 billion enterprise and automotive IoT endpoints by 2020, 2020. This example may be the most appropriate one: a woman's and her fetus' circulatory system to check on her health (Malik et al., 2018). In order to support the demanding and nondurable requirements of these novel applications, NB-IoT represents a practiced effort that enables lengthy distance communication at small data rates for sensors with little complexity and prolonged battery life. LPWAN enables industries to use existing BSs that are cellular and cover the entire establishing and the habitants of the spread. NB-IoT is also known one which has been used for this scenario. The healthcare system usually uses monitoring of sweating, respiratory rate, body temperature, and blood pressure that each sensor collects by sampling rates uttermost 2 Kbps (Malik et al., 2018). Another for rescue (Telenor Partner to Develop IoT Healthcare Devices 2020) and critical operations, together with the monitoring of important biotic signs, positioning according to GPS, motion sensors may be the necessary data rates of up to 200 Kbps (Alam and Ben Hamida, 2015a). The literature suggests a couple of notion in the current system of health surveillance as described below:

Single Sensor Node Design (Malik et al., 2018): Every sensor node is considered as a single detached node, and nodes have own communication module. As a result, all nodes transmit data on flat-out path to the BS with the proper requirements. The design presents several transmission links with the base station which are required for each patient.

Multi-Sensor Node Design (Malik et al., 2018): Different to single sensor node design, that is, all sensors are connected to a controller, in charge of processing the data and transmitting them to the base station. However, the design offers unique connection for each patient with the BS.

For the execution of the analysis of performance, standalone and in-band deployments use the peak bit rate of 180 kHz in a classical LTE cell. It is recognized for that the network is synchronized. The indistinguishable PRB in all cells is deployed for the network. Healthcare monitoring system has a traffic that is based upon lots of sensors with variations in information packet size and time interval. It is assumed that the patient is in critical state and needs constant monitoring. The performance of system is utilized in terms of prolificacy, supported device number, and delay.

Using the results of another work (Alam & Ben Hamida, 2015b) as a basis, different strategies for resource use can be also considered management in NB-IoT for healthcare application scenarios. Figure 3 shows type of system designs related to LPWAN.

3.2 Smart Agriculture Devices of NB-IoT

Food and Agriculture Organization (FAO) developed a concept on agriculture, food security and climate change at the 2010 Hague Conference. It is named as Climate Smart Agriculture (CSA). Thus, agriculture has gained a different importance and support with IoT. Smart agriculture covers ecological farming techniques and advanced methods of oversensitive farming apply information technology (IT) with the aim of optimization the use of water and other inputs. It is expected that smart agriculture has a potential beneficial effect on food and health etiquette (Agrimonti et al., 2020). With the progress of technology and industrial 4.0 indifferent areas, the linking of food information technology (Packer, 2020) and agriculture like as the IoT has spawned the application of intelligent agriculture (Singh et al., 2020a, b; Dubey et al., 2020; Sehgal et al., 2020; Padikkapparambil et al., 2020). The ingenious cloud-based agricultural data collection system (Skylo Ready to Launch Global NB-IoT Satellite-Based Network in Summer, 2020) and NB-IoT chiefly rely on the latest technology of the IoT to enhancement of its sensors monitoring network system for cultivation (Cannabis Industry Going High-tech to Improve Cultivation Operations, 2019), irrigation and growth environment and condition, as well as meteorological parameters. Cloud computing and NB-IoT-based smart farm information system use mainly the parameters such as air temperature and relative moisture, luminous intensity, pH value of irrigation water in plant protection systems, environment as a collection target for research and design. Today, it is becoming a time when agriculture is progressively shifting in direction of an era of facultative, localized, sophisticated, and highly efficient (SoftBank Deploys its AI-powered 'e-kakashi' Solution for Smart Rice Farming Project in Colombia, 2019). It can be based on modern science and technology to develop agriculture so that no one is needed to do service in the field, implement digital irrigation and make full use of the computer automatic control and software data systems to ensure reliable production. It can improve efficiency while steadily increasing financial yields. IoT projects in the agricultural are being contrived,

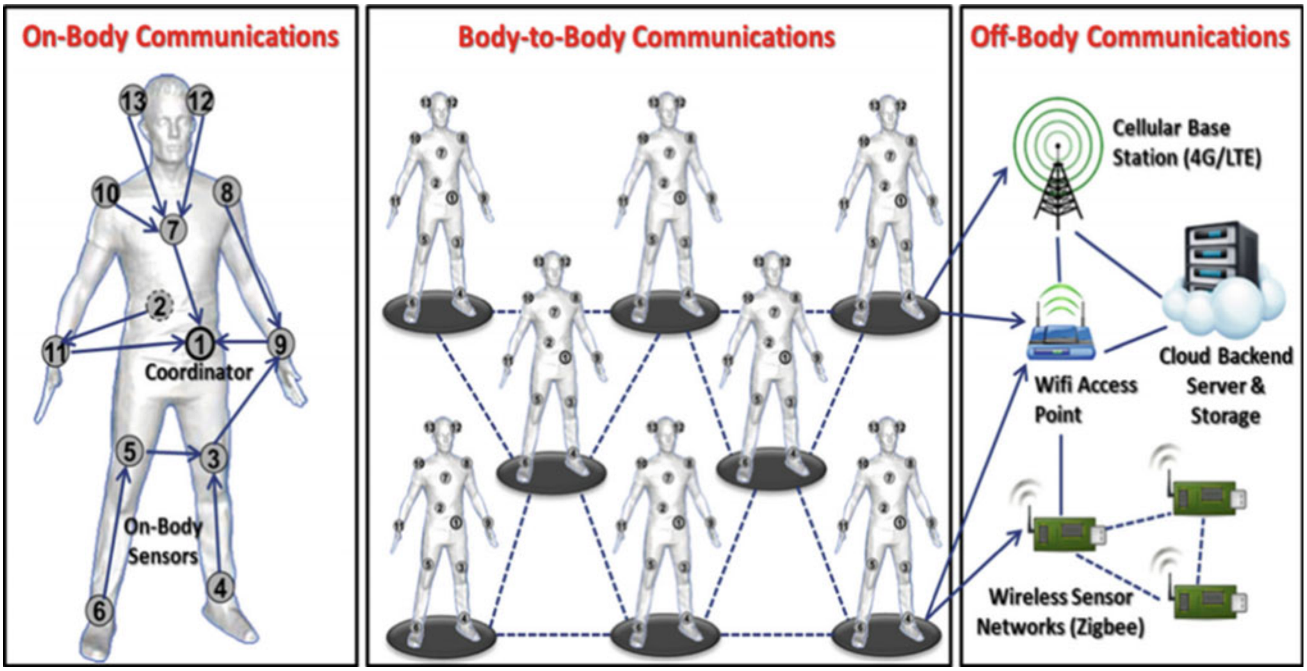


Fig. 3 On-body, body-to-body, and off-body wearable networks

which has many potential applications and room for expansion. It is the NB-IoT related cloud computing that fosters the growing of the tillage related innovations and builds up the support mechanism for rural development (Yao and Bian, 2020). Figure 4 demonstrates system structure of smart agriculture.

Livestock tracker and greenhouse sensors can be demonstrated as agriculture applications that utilize NB-IoT (Cengiz, 2015).

3.3 Livestock Tracker

NB-IoT-based small devices used by farmers to locate livestock like cows are known as livestock tracker. Updates about the location of the livestock are provided by system of NB-IoT. The device also provides own updates, like the level of battery. The data can be acquired using terrestrial and orbital technologies (Agriculture Using NB-IoT About The GSMA, 2018).

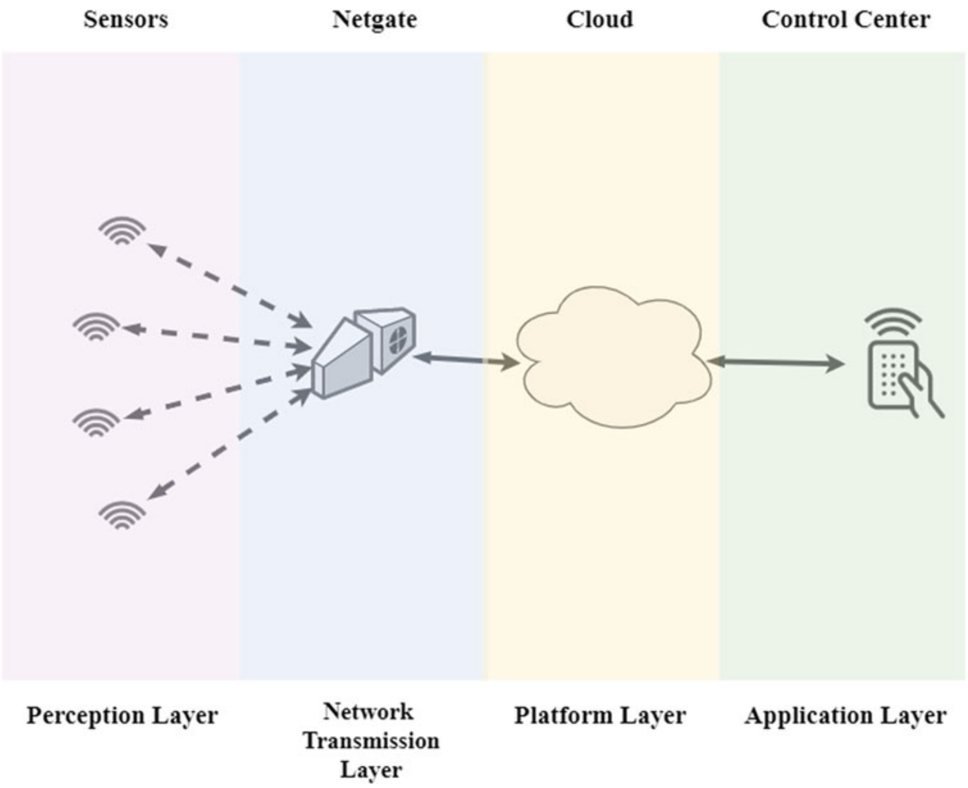
3.4 Greenhouse Sensors

We can get data of weather and climate events under favor of NB-IoT-based sensors. The system that has unique architecture also collects the both soil and air data. It monitors info about water. Thanks to sensors, productivity, and good conditions are ensured. It is because of alert system that warns the user (Agriculture Using NB-IoT About The GSMA, 2018). The data that is generated during process provides data for future predictions.

3.5 Pollution Detection in NB-IoT

The outraged pollution density in air threatens living creatures' health in world as we can see from space. And at present, air pollution is a major problem for mankind health in cities, which are among the more factors such as traffic, industrial or forest fire or polluted sky. Monitoring air quality statistics is important to render high-precision data. In 2020, although air pollution may have been going down for a bit (NPR, 2020), it is a danger anyhow for humankind and still harms climate, in the same breath (CNN, 2020). Those existing services that focus on air quality a smart city to monitor the strength of life, the weather monitoring, waste management, traffic management, energy consumption management (Cengiz & Dag, 2015), and also, the monitoring of air quality is very essential. The air quality index (AQI) is a descriptive method and an essential means for evaluating risks for public health. Numerous research projects are focused on the development of green technologies in the intelligent

Fig. 4 System structure of smart agriculture



cities. The limited access of data, the high expenditures, and the unscalability of the common air monitoring system force the world to focus on air pollution monitoring system using sophisticated technologies like IoT and wireless sensor network. The system that uses these technologies is called air pollution monitoring systems (APMS) (Idrees & Zheng, 2020). As in (Duangsuwan et al., 2018), WSN is widely used for environmental monitoring applications (Cengiz & Dag, 2016, 2018; Cengiz, 2016), and in Fig. 6, system architecture is shown. By using air pollution detection sensors, CO, O_3, NO_2, SO_2, and particulate matter are monitored and AQI can be evaluated.

3.6 Fog Computing in NB-IoT for Air Pollution Detection

The Cisco has proposed fog computing (Bonomi et al., 2012). Fog computing has a lot in common with cloud computing in many ways, such as the users of NB-IoT services such as data storage and processing. Fog is dispersed, as opposed to the cloud. A fog node can be any node that is not only connected to others but also having the memory, connectivity, and capacity of computational work. Figure 5 illustrates example of fog nodes working for pollution detection fog computing has three layers (Senthilkumar et al., 2020) (Fig. 6).

Device level: It forms the basis for the entire air quality monitoring system, and this is useful for preparing advisory in the first place. Because of these pathbreaking stuffs of the scanning stage, the air quality monitoring nodes are battery operated and installed over a large geographical area.

Fog: Fog computers (IoT gateways) are found in this layer. Each one has an intensely virtualization related applications and hosts on a pertained computer. Data collected by IoT devices is not immediately transferred to cloud to be operated. Before that, it may be transferred to another nodal point. Node can isolate data that not feasible and transfer them to the cloud for background analysis and prolonged vault.

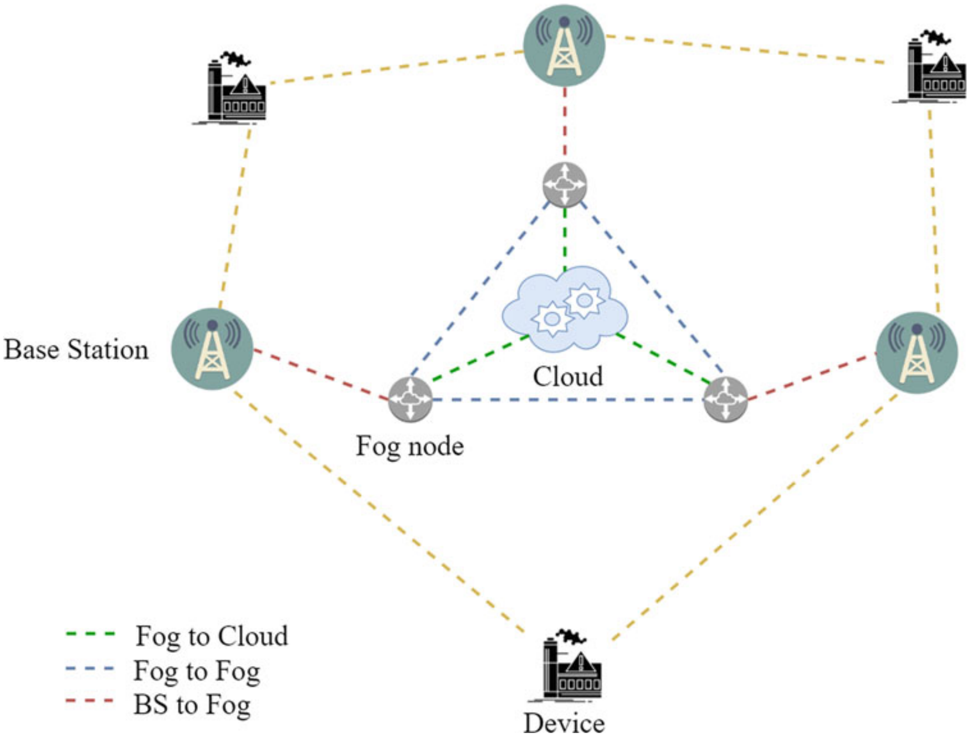
Cloud: This component is in charge of processing sensitive information plus deploys end-user support interactivity. At one occasion, cloud receives the data and keeps the data in own database, and it enables data presentation in a variety of formats.

Without noticing network terms, LPWAN can be seen as a key architecture for nature. Because it has a large area range and long battery life time, as a result, not only low cost and low power but also low throughput is a certain output for earth.

3.7 Intelligent Garbage Bin in Smart Cities

The garbage is a mandatory need in daily life and has passed through all eras of the social development of humanity. Today, it is particularly important in the urban environment. As people' awareness of the environment improves, the

Fig. 5 Fog computing



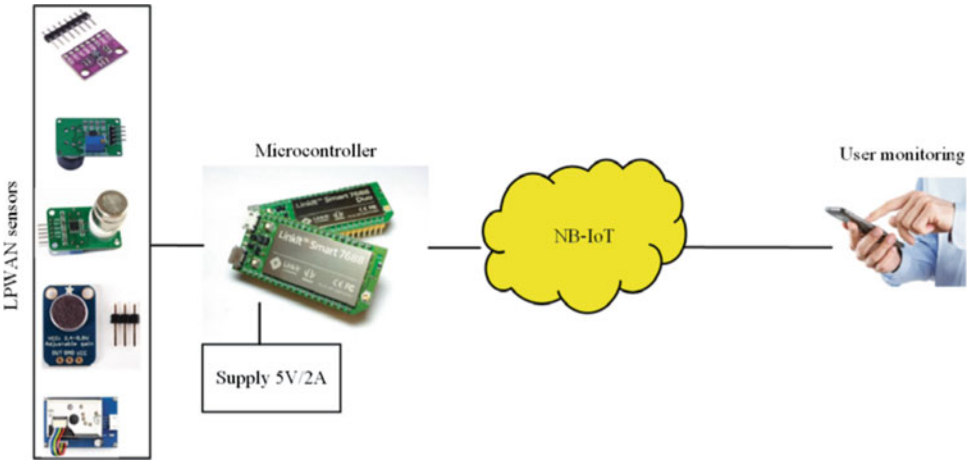


Fig. 6 Air pollution detection in NB-IoT

manner of the trash cans is evermore renewed. At present, trash problem for civilization is on a significant position. Traditional garbage cans rely on workers to control them. If they are full and need to be cleaned up, then workers have to handle that unaided. While collecting the garbage, they must go over the types of garbage in the bins manually. Reducing the caseload is a must. At present, a common rubbish bin has stinted doing and the new version of trash cans used has the handicap of deep manual handling. Yet, related research (Pan et al., 2019) is a kind as intelligent trash can and works with the NB-IoT technology. So that, it is not an ordinary trash can we are accustomed to. For the perception of things, infrared smell sensors are added to classify and recognize waste. The research is investigated through using chips on can which is different from an ordinary garbage can. It adds the waste can an Internet-based detector of things perception system, through scent sensors to attain assorted methods. Communication module is put to use for the transmission of information. And consequently, intelligent garbage can provide the sanitary workers with information, if the garbage gets full and if the garbage is toxic or not. Figure 7 illustrates the model drawing of garbage in (Pan et al., 2019). And Fig. 8 shows components of NB-IoT-based garbage bin.

3.8 Smart Parking

Road parking in the urbanized zones is stationary one that has the hallmarks of wider dispersion and atypical tightness. The situation of vehicular and insufficient parking spaces brings urban traffic congestion in its train. That issue becomes a significant challenger. For solving issues, the research (Shi et al., 2018) proposes a smart parking system was conducted. In the proposed plant, data from the nodes is transmitted by module, which is the technology introduced for LPWAN applications. Featuring an integrated refund substructure and parking directory vocation, the mobile application engineered for the vehicles are easy and useful to work with. Figure 9 shows related study. There are many reasons for the urban street's difficulties. Firstly, the car parking lot is serious insufficient, especially for the centrum. Second, the drivers cannot recognize status of the parking lot simultaneously. Thirdly, the traffic management department lacks parking data for strategic decisions simultaneously, too. Finally, the charging for parking is not handy, certainly not for the metering. Guiding the drivers to the nearest parking spaces and making the payment simple is the hot potato of this field.

3.9 Fog Computing Approach for Smart Parking

With fog computing, the cloud computing instance is extended to the brink of the network paradigm. A fog node can be seen as a small capacity counterpart to a cloud that employs the same resources such as networking, but there is a crucial distinction between the fog node and the cloud server from application demand when low latency, large connections, geographically distributed sensor networks and agile mobile devices such as intelligent attached trucks are the relevant metrics of performance.

Taiwan's major security service providers have had a collaborative commercial trial project. The architecture of the intelligent parking system is demonstrated in Fig. 10. With the proposed system, a NB-IoT sensor is allocated to individual parking spaces with unique identifier like an eSIM. In addition, to access the parking service, all vehicles that use parking lot must be equipped with a tracker given by service provider.

The system works as follows. First, the parking space sensors remain off until a vehicle comes near. Next, the NB-IoT sets off and starts its act as standby mode. After, it waits for the parking the sensor to link between the vehicle and the parking space. As other sensors in neighboring parking spaces are in standby mode, the tracking sensor

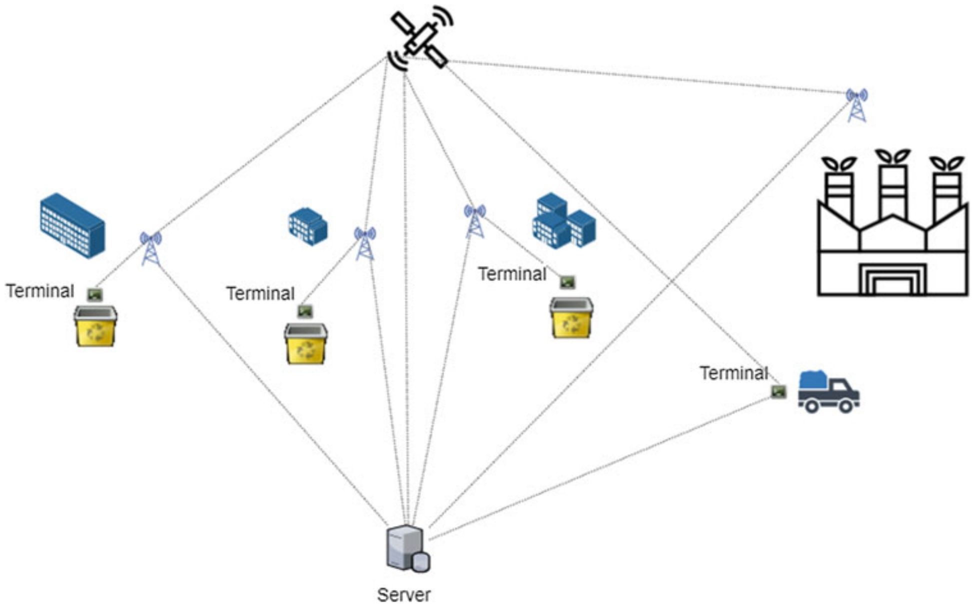


Fig. 7 Basic relationship between terminals, server and base stations in Smart Garbage scenario

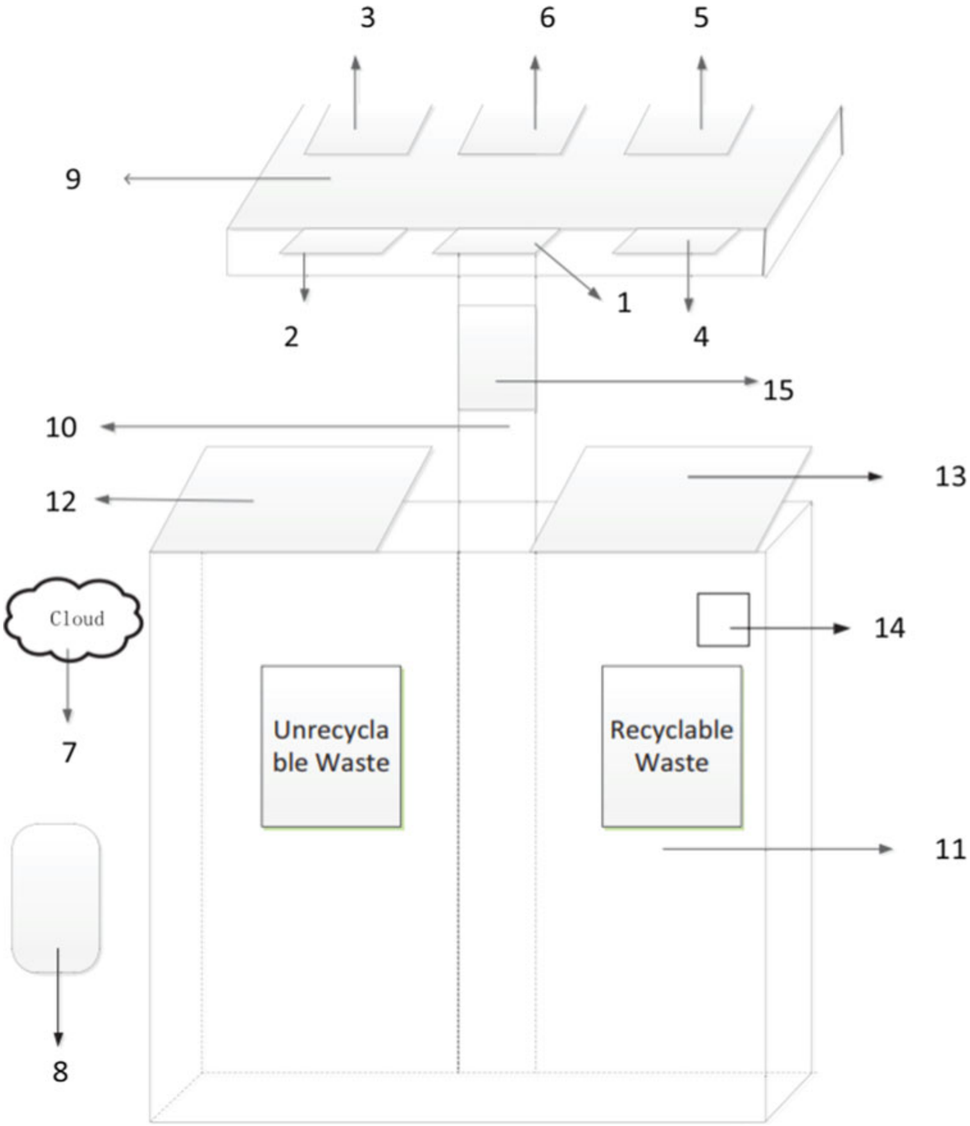


Fig. 8 1 (single-chip microcomputer) 2 (infrared sensors) 3 (air quality detector) 4 (odor sensor) 5 (NB-IoT communication module) 6 (solar panels) 7 (cloud servers) 8 (mobile terminals) 9 (garbage box top cover) 10 (top cover support column) 11 (dustbin) 12 (left lid of dustbin) 13 (right lid of dustbin) 14 (buzzer) 15 (LED)

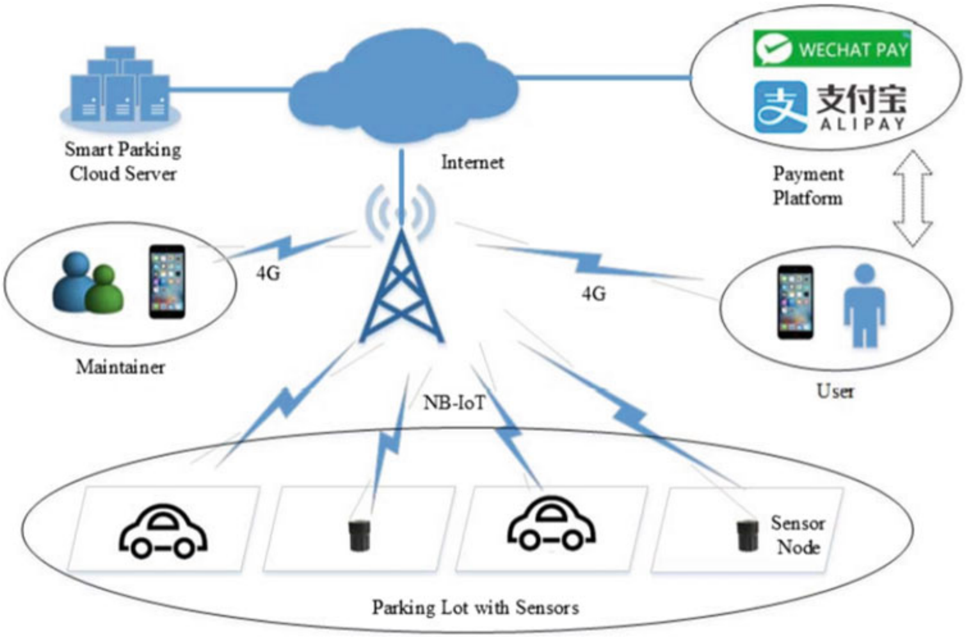


Fig. 9 Overview of network system for smart parking

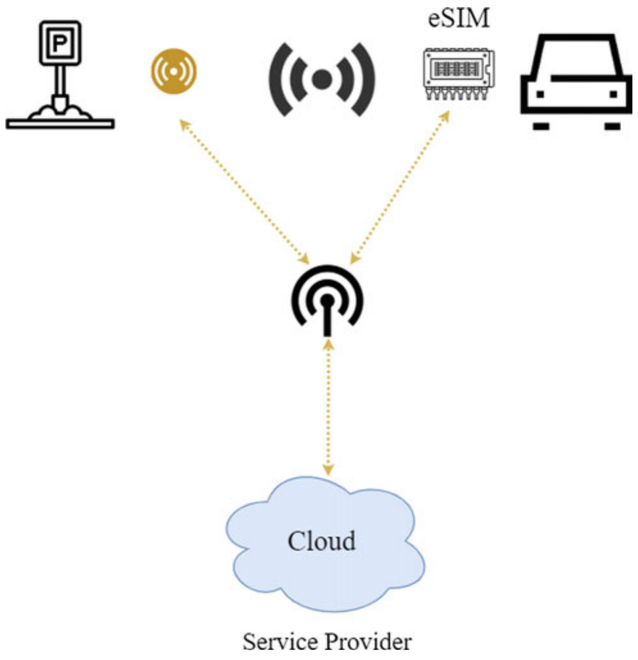


Fig. 10 Service provider manages the scenario through the cloud

could just connect to a single sensor that is just under the vehicle. When the connection success, all the information that the vehicle has will be forwarded to the cloud. As the car departs, a typical process happens.

3.10 Smart Factory

The main and essential ingredients of Industry 4.0 are information and object connectivity (Cengiz et al., 2020). The fourth industrial revolution for factories is the broad use of smart agents and sensors to network components, operators and processes as well as machines. These abilities let the factories produce more wisely and manage the progress with no mistake. If the factories are not making a mistake, the reason is powerful communication as well. Communication for factories in twenty-first century is involved in Industrial Internet of Things (IIoT) (Tanwar, 2020a, b; Vora et al., 2017; Gupta et al., 2020). As we know, IoT needs WSN to pursue its impact. It gets us free of wires in factories. Increasing competition on the market is bringing a new production way plus an emphasis on the smart factories from all viewpoints. The most of smart factory approaches is suggested and trialed. The investments for a smart factory technology must also be determined and proven to be economically justifiable edgy. The study (Lu et al., 2018) captures the characteristics of the smart factory as being data-driven, with widely distributed network and on top, data is continuous and repetitively used to improve the production, human-free. But modern-day production structure is made up of complicated and complex production systems due to a myriad of determinants that can vary from a special fabric.

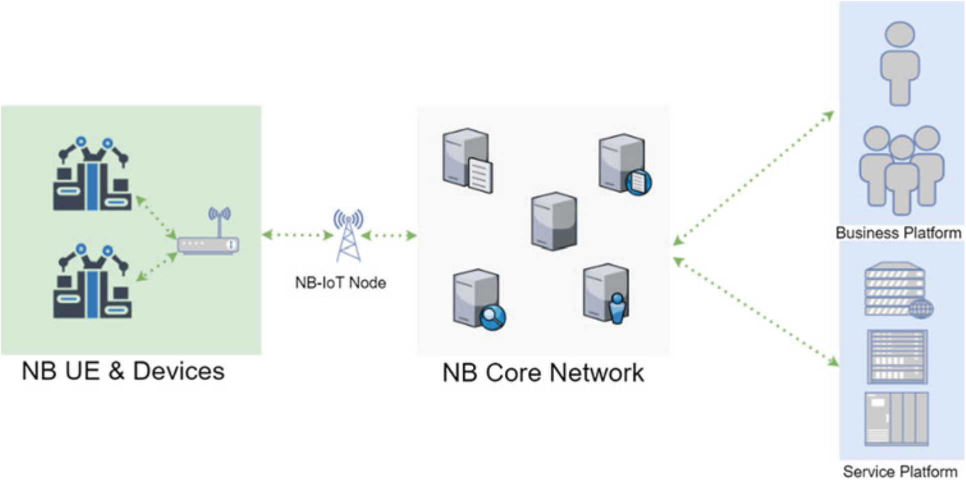


Fig. 11 Topology of smart factory in China

Fig. 12 Measuring locations in Svanemoellehavn

3.11 OneNet Platform

In China, OneNet platform of the China Mobile (CMCC) is a widely eminent and mature setup for business-to-business trade and business-to-consumer companies. It is an application enable platform (AEP), and it has IoT scenario applications. These applications include extensive computer simulations, intelligent memory block loading and related APIs. There is no doubt that the architecture of the OneNet project is blazing, elements such as the equipment, application, triggers of events, and data stream are arranged by the customers' designs, and the feedback for every is planned to be initiated by actions and resulting from predetermined claims (Fig. 11).

3.12 NB-IoT for Maritime Use Case

A marine environmental signal strength and other released inputs must be suitable. Accordingly, the primary uses for NB-IoT incur the mass category of IoT, of which device number, electricity usage and network range take on a significance title than delay or pace of data transfer. The purpose of the study (Malarski 2018) is to solve the question of whether the NB-IoT was workable in the maritime transport case. So, NB-IoT has been conducted as harbor monitoring system make a show of experiment. Figures 12, 13, and 14 illustrate information about the study.

Container traffic involves over 90% of world trade, and there are along trade routes, both sea and land (Katulski et al., 2009). There are many industrial companies that actually monitor containers at sea. Maersk is one of them. It uses satellites to give out the data collected from its intelligent containers (New Maersk Smart Containers Can Listen and Talk, 2016). Thanks to GPS, during a SIM card or a modem allow to collect, store, and share meteorological events and power state. Using GPS means also that LOS is not an obstacle for shipping companies. In (Cluzel, 2018), the paper discusses the broadening of the outreach of LPWAN-based low earth orbit (LEO) satellite configurations. Yet, with all the advantages of this method, it carries a

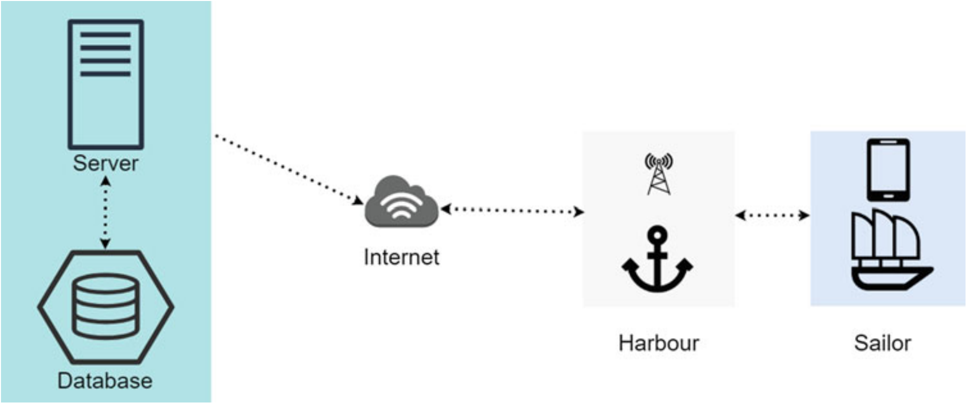


Fig. 13 Harbor monitoring system showing device scenario

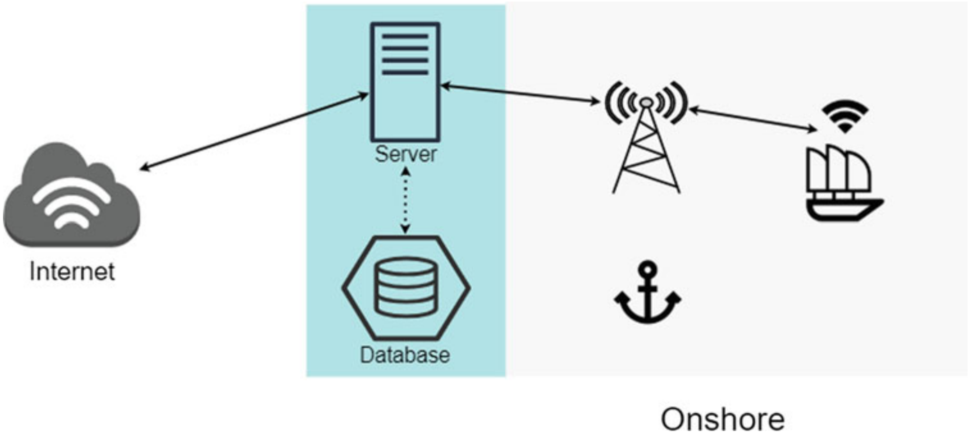


Fig. 14 Harbor monitoring system showing sensor mode of operation

high risk. Most of the time, the containers are locked while the shipping to keep the load on the inside of them outside of any control. In this condition, it is the critical oversight and monitoring issue of the cargo container, both during transport and stored.

4 Conclusions

IoT and its novel version NB-IoT use intelligent networks to meet the requirements of the modern world. These technologies are very significant for gathering data from the environment and real-world applications. Mobile networks such as 3G and 4G were designed to be used for voice, data, and video transmissions. However, nowadays, 5G mobile networks aim to solve the issues of existing cellular technologies and to be a potential key factor for the future IoT. In this chapter, we aim to present the role of IoT and NB-IoT for several use cases such as intelligent health care for people, smart agriculture devices of NB-IoT, livestock tracker, greenhouse sensors, pollution detection in NB-IoT, fog computing in NB-IoT for air pollution detection, intelligent garbage bin in smart cities, smart parking, fog computing approach for smart parking, smart factory, OneNet platform and NB-IoT for maritime use case. For future studies, we aim to generate novel solutions to IoT and NB-IoT technologies in healthcare applications.

References

Agriculture Using NB-IoT About The GSMA. (2018). https://www.gsma.com.

Agrimonti, C., Lauro, M., & Visioli, G. (2020). Smart agriculture for food quality: facing climate change in the 21st century. *Critical Reviews in Food Science and Nutrition*. Taylor and Francis Inc. https://doi.org/10.1080/10408398.2020.1749555.

Air Pollution Levels Down Only Slightly Since the Coronavirus: Short Wave: *NPR*. (2020) https://www.npr.org/2020/05/27/862920439/the-pandemic-cut-down-car-traffic-why-not-air-pollution.

Alam, M. M., & Ben Hamida, E. (2015a, September) Strategies for optimal MAC parameters tuning in IEEE 802.15.6 wearable wireless sensor networks. *J. Med. Syst.*, *39*(9), 1–16. https://doi.org/10.1007/s10916-015-0277-4.

Alam, M. M., & Ben Hamida, E. (2015b, September). Strategies for optimal MAC parameters tuning in IEEE 802.15.6 wearable wireless sensor networks. *Journal of Medical Systems, 39*(9), 1–16. https://doi.org/10.1007/s10916-015-0277-4.

Aydemir, M., & Cengiz, K. (2017, July). Emerging infrastructure and technology challenges in 5G wireless networks. In 2nd *International Multidisciplinary Conference on Computer and Energy Science (SpliTech2017)*, Split, Crotia.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *MCC'12 - Proceedings of the 1st ACM Mobile Cloud Computing Workshop* (pp. 13–15). https://doi.org/10.1145/2342509.2342513.

Cannabis Industry Going High-tech to Improve Cultivation Operations. (2019). https://www.prnewswire.com/news-releases/cannabis-industry-going-high-tech-to-improve-cultivation-operations-300849423.html.

Cellular and LPWA IoT Device Ecosystems 2020-2024-ResearchAndMarkets.com | Business | The Daily News. (2020). https://www.galvnews.com/news_ap/business/article_b2e352ac-1452-5518-99ef-6e45ebd616bf.html.

Cellular IoT Market by Offering (Hardware and Software) Market Growing Trends and Technology forecast 2020 to 2026. 3w Market News Reports. (2017). https://3wnews.org/uncategorised/1496830/cellular-iot-market-by-offering-hardware-and-software-market-growing-trends-and-technology-forecast-2020-to-2026/.

Cengiz, K. (2015). Towards green communications. *Advances in Wireless Communications and Networks, 1*(1), 1–5. https://doi.org/10.11648/j.awcn.20150101.11.

Cengiz, K. (2016). Constant clustering with nearest cluster heads in WSNs. *International Journal of Computer Science & Engineering Technology, 7*(11), 463–468.

Cengiz, K., & Aydemir, M. (2018). Next-generation infrastructure and technology issues in 5G systems. *Journal of Communication Software and Systems (JCOMSS), 14*(1).

Cengiz, K., & Dag, T. (2015). A review on the recent energy-efficient approaches for the Internet protocol stack. *Eurasip Journal on Wireless Communications and Networking*, 108. https://doi.org/10.1186/s13638-015-0336-z.

Cengiz, K., & Dag, T. (2016). Improving energy-efficiency of WSNs through LEFCA. *International Journal of Distributed Sensor Networks, 8*(12), 8139401. https://doi.org/10.1177/155014778139401.

Cengiz, K., & Dag, T. (2018, February). Energy aware multi-hop routing protocol for WSNs. *IEEE Access Journal*, *6*(2018-10600), 2622–2633. https://doi.org/10.1109/access.2017.2784542.

Cengiz, K., Sharma, K., Kottursamy, K., Singh, K. K., Topac, T., & Ozyurt, B. (2020). Recent emerging technologies for intelligent learning and analytics in big data. *Multimedia Technologies in the Internet of Things Environment*, Studies in Big Data, Springer, Berlin (Under Press).

Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrow band Internet of Things. *IEEE Access, 5,* 20557–20577. https://doi.org/10.1109/ACCESS.2017.2751586.

Cluzel, S., et al. (2018). 3GPP NB-IOT coverage extension using LEO satellites. In *IEEE Vehicular Technology Conference*, July 2018, (Vol. 2018, pp. 1–5). https://doi.org/10.1109/vtcspring.2018.8417723.

Connected world gives greater supply chain visibility | Packer. (2020). https://www.thepacker.com/article/connected-world-gives-greater-supply-chain-visibility.

Duangsuwan, S., Takarn, A., Nujankaew, R., & Jamjareegulgarn, R. (2018). A study of air pollution smart sensors LPWAN via NB-IoT for Thailand Smart Cities 4.0. In *2018 10th International Conference on Knowledge and Smart Technology: Cybernetics in the Next Decades*, KST 2018 (pp. 206–209). https://doi.org/10.1109/kst.2018.8426195.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Ericsson, Sony, and Telenor Partner to Develop IoT Healthcare Devices. (2020). https://www.rtinsights.com/sony-ericsson-telenor-iot-wearables/.

Gartner sees 5.8 billion enterprise and automotive IoT endpoints by 2020. (2020) https://futureiot.tech/gartner-sees-5-8-billion-enterprise-and-automotive-iot-endpoints-by-2020/.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Idrees, Z., & Zheng, L. (2020). Low cost air pollution monitoring systems: A review of protocols and enabling technologies. *Journal of Industrial Information Integration, 17,* 100123. https://doi.org/10.1016/j.jii.2019.100123.

Katulski, R., Sadowski, J., Stefański, J., Ambroziak, S., & Miszewska, B. (2009). Self-organizing wireless monitoring system for cargo containers. *Polish Maritime Research, 16*(3), 45–50. https://doi.org/10.2478/v10012-008-0033-5.

Lu, Y., Zhou, Y., Tong, E., Ding, F., & Wu, J. (2018, July). Performance and cost analysis of an NB-IoT based smart factory solution with OneNet cloud. In *2018 2nd International Conference on Imaging, Signal Processing and Communication*, ICISPC 2018, July 2018 (pp. 120–124). https://doi.org/10.1109/icispc44900.2018.9006674.

Malarski, K. M., et al. (2018). Demonstration of NB-IoT for maritime use cases. In *Proceedings of the 2018 9th International Conference on the Network of the Future*, NOF 2018, December 2018 (pp. 106–108). https://doi.org/10.1109/nof.2018.8598067.

Malik, H., Alam, M. M., Le Moullec, Y., & Kuusik, A. (2018). NarrowBand-IoT performance analysis for healthcare applications. *Procedia Computer Science, 130,* 1077–1083. https://doi.org/10.1016/j.procs.2018.04.156.

New Maersk Smart Containers Can Listen and Talk. (2016). https://www.dynamicexport.com.au/freight/articles-freight-and-insurance/New-Maersk-smart-containers-can-listen-and-talk.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 217–243). Academic.

Pan, P., Lai, J., Chen, G., Li, J., Zhou, M., & Ren, H. (2019). An intelligent garbage bin based on NB-IOT research mode. In *Proceedings of 2018 IEEE International Conference of Safety Produce Informatization*, IICSPI 2018 (pp. 113–117). https://doi.org/10.1109/iicspi.2018.8690408.

Sales of Cellular Iot Market to be Significantly Influenced by Rising Consumer Adoption. Cole Reports. (2020). https://coleofduty.com/technology/2020/06/05/sales-of-cellular-iot-market-to-be-significantly-influenced-by-rising-consumer-adoption/.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Senthilkumar, R., Venkatakrishnan, P., & Balaji, N. (2020). Intelligent based novel embedded system based iot enabled air pollution monitoring system. *Microprocessors and Microsystems, 77,* 103172. https://doi.org/10.1016/j.micpro.2020.103172.

Shi, J., Jin, L., Li, J., & Fang, Z. (2018, January). A smart parking system based on NB-IoT and third-party payment platform. In *2017 17th International Symposium on Communications and Information Technologies*, ISCIT 2017, July 2017, (Vol. 2018, pp. 1–5). https://doi.org/10.1109/iscit.2017.8261235.

Siberia's prolonged unusually warm weather is an 'alarming sign': scientist says. *CNN.* (2020). https://edition.cnn.com/2020/06/18/europe/siberia-warming-climate-crisis-intl-hnk/index.html.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of Things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth, 2,* 191.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020b). Internet of Things in pharma industry: Possibilities and challenges. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 195–216). Academic.

Skylo Ready to Launch Global NB-IoT Satellite-Based Network in Summer 2020 | Light Reading. (2020). https://www.lightreading.com/iot/skylo-ready-to-launch-global-nb-iot-satellite-based-network-in-summer-2020/d/d-id/756945.

SoftBank Deploys its AI-powered ‘e-kakashi’ Solution for Smart Rice Farming Project in Colombia. (2019). https://www.thefastmode.com/technology-solutions/15827-softbank-deploys-its-ai-powered-e-kakashi-solution-for-smart-rice-farming-project-in-colombia.

Tanwar, S. (2020a). *Fog computing for healthcare 4.0 environments: Technical, societal, and future implications, signals and communication technology*. Springer International Publishing (pp. 1–622).

Tanwar, S. (2020b). Fog Data Analytics for IoT applications—next generation process model with state-of-the-art Technologies. *Studies in Big Data, 76*, 1–497. (Springer International Publishing).

Vora, J., Tanwar, S., Tyagi, S., Kumar, S., & Rodrigues, J. J. P. C. (2017). Home-based exercise system for patients using IoT enabled smart speaker. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian (pp. 1–6).

Yao, Z., & Bian, C. (2020). Smart agriculture information system based on cloud computing and NB-IoT. DEStech Transactions on Computer Science and Engineering (cisnrc). Accessed June 20, 2020. [Online]. Available http://www.dpi-proceedings.com/index.php/dtcse/article/view/33340.

Robust and Secure Routing Protocols for MANET-Based Internet of Things Systems—A Survey

Rajvi Trivedi and Pimal Khanpara

Abstract

In recent decades, the Internet of things (IoT) has had a huge impact on various domains, such as logistics, health care, robotics, and manufacturing, coping with an enormous amount of data transferred by different resource-constrained IoT network devices. For diverse applications, IoT can be seen as a network of devices comprising hardware, software, sensors, actuators, and connectivity allowing the networked system to link, communicate, and share information. In IoT configurations, billions of devices can be connected to the Internet to transfer data quickly, efficiently, and securely. Though there are great advancements in IoT technologies, certain limitations are still to be considered. Firstly, IoT devices have limited resources like memory, computing power, and energy (Khanpara and Lavingia in Multimedia big data computing for IoT applications. Springer, Singapore, pp. 37–57, 2020). Besides, IoT devices may link the behavior of a person to their identity which challenges the privacy of a person. Many researchers have made numerous successful attempts to integrate reliable protocols with IoT devices that can function efficiently in a resource-constrained environment and robustly against data transmission security and privacy issues. IoT integrates with the wireless sensor network (WSN) and the mobile ad hoc network (MANET) in smart environments and is becoming much more desirable and economically efficient. The MANET is not only ideal for disaster situations but can also be used for robotic communication. Interaction with the IoT systems between WSNs and MANETs enables the development of new MANET-based IoT systems which give the consumer more mobility and lower costs. At the same time, the networking aspects open up new challenging issues. Hence, this chapter discusses various existing secure MANET protocols that provide secure data transmission and can also be used in the IoT environment to provide robustness in the presence of a variety of threats and vulnerabilities. This chapter also presents some major challenges in the emerging domain of MANET-based IoT systems for robotics.

Keywords

Cyber-physical systems (CPSs) • Internet of Things (IoT) • Mobile ad hoc networks (MANETs) • Wireless sensor networks (WSNs) • Routing • Network security • Robotics

1 Introduction

With the increase in the development of wireless sensor networks, a wide range of IoT applications have also got a huge breakthrough. There are various domains and prospects of developments in IoT applications such as intelligent medical treatments, robotic instruments, environment monitoring, smart grid, transport systems, and many other areas (Zhao & Ge, 2013). IoT architecture is combined with various devices and technologies such as sensors, actuators, data sources, Radio Frequency Identification Device (RFID), device control, edge processing and analytics, global positioning system (GPS), data integration and routing, and application development. IoT has globally emerged as an interrelated network system through sensors which collect data in real-time, then send it to processors via edge or/and cloud technology to a server, and the server then processes this data and sends it to the actuator and applications to analyze the data and react accordingly. The system collects a variety of information such as light, heat, sound, electricity, biology, location, and others. This indicates the possible IoT connection patterns that are machine to machine, machine to man, and man to man. In one

R. Trivedi (✉) · P. Khanpara
Institute of Technology, Nirma University, Ahmedabad, India
e-mail: rajvitrivedi31@gmail.com

P. Khanpara
e-mail: pimal.khanpara@gmail.com

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_12

of the tech reports of Goldman Sachs, it was mentioned that by the year 2020, more than 2.8 zillion of things will be connected by the Internet (Sachs, 2014).

The Internet of things (IoT) considers a diversity of things to be prevalent in the environment. Through wireless and wired links and distinctive addressing schemes, things can communicate and collaborate with one another to develop new applications/services as well as work toward common goals. The Internet of things as a network of interconnected things incorporates multiple technologies for interacting and perceiving or communicating with their internal or external states. The integration of effective wireless protocols, enhanced actuators, affordable processors, necessitates the synergies produced by end user, commercial enterprise, and Industry 4.0 integration to be used. The integration creates a global, open network that links people, data as well as objects. It deploys the cloud to link smart things that detect and communicate a wide quantity of information, helping to build solutions that would not be readily apparent without such a level of communication and scientific competence (Tanwar, 2020). Groundbreaking advancements such as the cloud, objects, and smartphones propel the use of systems.

Cyber-physical systems (CPS) (Gupta et al., 2020) depict the next generation of embedded intelligent ICT systems which are interrelated, intertwined, cooperative, self-reliant and that offer computing and communication, tracking/ control of physical devices/processes in different application areas. Potential CPS needs to be scalable, distributed, decentralized, enabling people, ecosystems, and devices to communicate while connecting to the Internet or other networks. Adaptability, reactivity, optimality, and security are characteristics that must be integrated into such systems, as the CPS is now forming an unseen society's 'neural network' of the community.

With recent advancements in the Internet, the way of living for people has been enhanced. The Internet of All (IoE) envisaged all facets of getting people together and connecting to the physical world. It has since surfaced in several ways that had never before been envisioned. Cyber-physical systems (CPSs), big data (BD), and the Internet of things (IoT) concept are intended to use more powerful people-to-people connections to support the future of connectivity and reachability. There are a wide range of areas where such solutions have full ability to facilitate a modern lifestyle, along with production, transportation, health care, waste disposal, water management, farming, factory automation, robotic systems, automatically controlled aviation, independent engineering and manufacturing systems, and so on. To communicate with things locally and globally, both disciplines incorporate and implement intelligent devices, a physical world's interaction, and individuals to connect with each other completely (Padikkapparambil et al., 2020). The Internet advancements have completely flipped the way we live and work, how we perform, and how we acquire the knowledge in a very short period of time. IoT and CPS perception proposes a world that brings each object digitally and automatically together while providing seamless interactions between Internet services and physical elements. As per a research, CPSs implement an IoT paradigm in order to provide the services that use the Internet for further processing and control and accessibility (Singh et al., 2020a; Dubey et al., 2020).

IoT is nowadays considered as one of the highest escalating research questions among the different intersection principles of five research domains such as nomadic computing, wireless sensor networks, cyber-physical systems, ubiquitous, and IoT (Singh & Kumar, 2020). Growing demand and rapid development of IoT system applications and domain technologies need real-time connectivity with robust threat protection security.

In this chapter, we describe various existing secure MANET protocols that provide secure data transmission and can also be used in the IoT environment to provide robustness in the presence of a variety of threats and vulnerabilities. The objective is to critically analyze the existing security in routing solutions applying MANET-connected communication system of IoT. The present research difficulties in implementing robust routing protocols for MANET-based IoT systems are also discussed in this work (Deepika & Anand, 2013; Dhiman & Nayyar, 2013).

A MANET creates the network dynamically and establishes the packet transmission path temporarily, because of that it is known as an infrastructure-less network. In a MANET structure, there is not any centralized or fixed infrastructure administration, but a bunch of mobile hosts contains wireless network interfaces from a temporary network. In a MANET network, the wireless nodes which are in transmission range can communicate in each direction, but for the nodes which are outside the range, communication needs to rely on other in-between wireless network nodes to send/receive packets (Perkins, 2001). Due to this, when the source and destination nodes are far away then a multi-hop scenario is created. In this case, there are multiple intermediate nodes on which the sender and receiver nodes need to rely, to send, and/or receive the messages. In this scenario, the intermediate nodes act as routers. In multi-hop nodes communication systems, the success rate strongly depends on the cooperation of other nodes. The attributes of all participating nodes which affect the multi-hop system are packet transmission power levels, nodes movement, coverage patterns of transmitter/receiver, and the interference level of co-channel. In such circumstances, the network topology keeps changing with time; when the source, intermediate, and/or destination node's position changes (Wu et al., 2007).

Connectivity and security are very important for any routing protocol which provides wired and wireless network communication services. So, the success of MANETs also highly depends on the steady connectivity and trustworthy security. However, MANETs prove both challenges and success in implementing and achieving the security goal via various characteristics of routing protocols, such as confidentiality, authentication, integrity, non-repudiation, availability, and access-control. As we already discussed, in MANETs, the nodes must follow the nature of strict cooperation to participate as mobile hosts. A variety of security techniques are developed for MANETs. Also, many security-enhancing protocols are proposed to enforce the cooperation characteristics and prevent the network from misbehavior; examples are ARAN, SSL, CONFIDENT, SAODV, 802.11 WEP, and many more. Though, none of these protocols are able to prevent/defend the network against all possible attacks (Khanpara & Trivedi, 2017; Khanpara 2018). Hence, in MANETs, the second line of defense called an intrusion detection system (IDS) is required to be applied, because IDSs are popular in some of the latest security tools against the battle of attacks (Khanpara & Trivedi, 2018; Shah & Khanpara, 2019). Researchers have also introduced the idea of distributed IDSs for MANETs to monitor network nodes' selfishness and/or misbehavior. Based on the information collected from the network behavior, subsequent actions can be determined to strengthen the security in network communications (Wu et al., 2007; Khanpara & Trivedi, 2018). In this chapter, we describe how existing MANET routing protocols can be used in the IoT environment to ensure the security of communication process. The remainder of this paper is organized as follows: Section 2 explains how the routing protocols defined for MANETs are useful for a variety of applications in the IoT domain. Section 3 discusses the existing, secure MANET routing protocols that are compatible with the communication process required for the IoT systems. A detailed analysis of such existing protocols is also presented in Section 3. Section 4 describes the major challenges and research directions with some concluding remarks for the proposed work.

2 MANET-Based Routing in IoT Systems

Many IoT systems use the MANET-based routing because there are a very few IoT-specific routing protocols exist which are evaluated by the IETF working group. MANET routing protocols for the IoT systems are usually analyzed based on the low-power and lossy network characteristics.

An IoT system comprises different devices and nodes that communicate with one another, consume the shared network resources, and can be a part of either the same or different MANETs. IoT devices that are connected through a MANET network can communicate with the IoT device nodes and other MANET routing supported IoT nodes and even with other non-MANET nodes. IoT devices and MANET network nodes require efficient and reliable routing methods in the existing MANET topology, for example, the routing methods that are proposed in (Bruzgiene et al., 2017) using MANET protocols can be associated with either IoT devices or can be treated as controllers for the connected IoT devices. MANET topology structure clusters are formed dynamically in its wireless radio range and then the cluster heads are selected for each cluster. The other cluster nodes (non-cluster head) in the network, forward data to their cluster heads within a fixed radio range. Cluster members communicate only with their cluster members and the cluster head. This way, cluster members only communicate and send data to their cluster heads and the cluster heads are responsible for data gathering, transmitting, and aggregating from their cluster members.

Based on the given application's requirements, MANET-connected IoT devices need different communication methods to secure the process of routing. Possible scenarios for the same are described in Table 1. This table mainly describes the probable ways to use MANETs in the communication of IoT devices in a secure manner. Some examples of the possible MANET-IoT connections are IoT devices connected to MANET nodes, IoT devices as a MANET node, IoT device may directly be connected to the Internet node, IoT device connected to more than one MANETs, and MANET nodes connected to IoT devices, Internet nodes or non-IoT nodes.

MANET routing protocols are generally classified into three categories of routing mechanisms: (1) reactive (known as on-demand), (2) proactive (known as table-driven), and (3) hybrid (uses the good features of both the reactive and proactive mechanisms) (Khanpara et al., 2010; Khanpara, 2014). These categories are defined in Fig. 1 based on the routing information acquiring methods and maintenance of the routing-related information. Reactive routing is the on-demand routing method that finds the route based on the demand which leads to flooding the network with routing requests for setting up the communication path. If the IoT system nodes are mobile, then it is beneficial to use reactive routing techniques. Nodes in the proactive routing need to maintain up-to-date lists of the routes (Nayyar, 2012). Due to dynamic topology and mobility of nodes, when the network nodes are fixed and steady, the proactive routing method is more suitable. The hybrid routing methods provide the benefit of both reactive as well as proactive routing. In hybrid routing techniques, routing is initially established using proactive routing techniques, and then reactive routing such as flooding is used for route establishment and maintenance (Abusalah et al., 2008a; Singh, 2011).

Many security threats and vulnerabilities exist in the MANET routing procedure, and hence, it is required to

Table 1 IoT connected device communication options

	Communication method									
Network connectivity with IoT devices	IoT device connected to MANET node	IoT device itself is a MANET node	IoT device connected to the same MANET node	IoT node connected to another node in the same MANET	IoT device connected to another MANET node	IoT device connected is another MANET node	A node in the same MANET network	A node in another MANET network	Non-IoT MANET node	Non-IoT Internet node
To a MANET node			√	√	√	√	√	√	√	√
Is a MANET node				√	√	√	√	√	√	√
To an Internet node	√	√							√	
Is an Internet node	√	√							√	

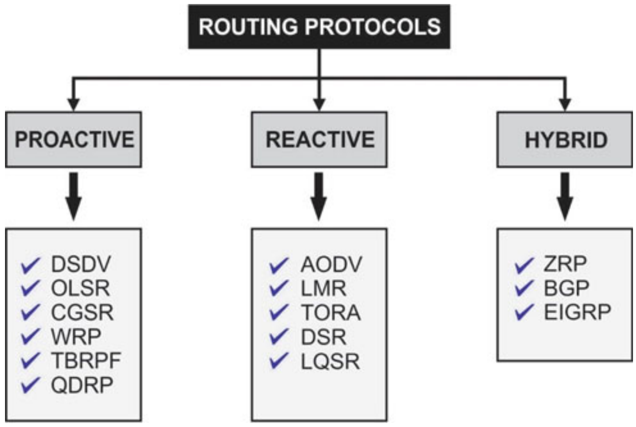


Fig. 1 Types of routing protocols (http://www.computerscijournal.org/wpcontent/uploads/2017/03/Vol10_No1_Com_Sac_Fig1.jpg)

enhance the security in routing protocols by designing the model as the methodologies for supporting the security routing.

IoT devices use different MANET protocols which help the system to connect to the network securely. These MANET protocols are trusted by the Internet Engineering Task Force (IETF) and verified for Internet standards of the routing protocols (Karlsson et al., 2018). IoT devices in the system connected via MANET nodes for the routing purpose are typically Low-power and lossy network (LLN). Specifically, for the routing purpose in the IoT system devices, the IETF working group proposed the routing protocol named routing protocol for low-power and lossy network (RPL) (Request for Comments (RFC) 4944, IETF, 2007; RPL, 2012). RPL routing protocol is a distance vector-based IPv6 routing protocol. In RPL, the routing paths have the LLNs nodes and these nodes are organized such that it can behave as a set of destination-oriented directed acyclic graphs (DODAG). These DODAGs consist of IoT device nodes and sink nodes that can collect data from the IoT device nodes. The architecture of the RPL protocol and the behavior of IoT devices are shown in Fig. 2. This figure shows how the RP router interfaces and/or the other LLN routing are connected to the IoT devices and communicating with the Internet host. Also, other IoT devices can connect and communicate if they are in the same LLN (Airehrour et al., 2016).

2.1 Requirements of Secure Routing Protocols in IoT

The fundamental requirements of the secure routing process for the wireless networked systems such as IoT and robotics are listed below:

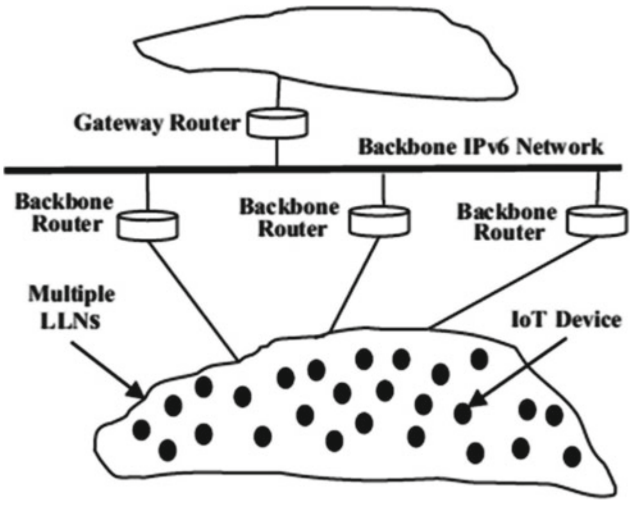


Fig. 2 Network architecture for IoT devices connected to LLN (Karlsson et al. 2018)

Malicious Nodes Detection: It is required that a proposed routing protocol is able to detect the presence of malicious nodes in the network and also able to avoid the participation of this kind of nodes in the network during the routing process. There must be some mechanism such that even if the malicious nodes enter into the route discovery process, paths containing malicious nodes should not be selected as routes for data transmission (Karthigeyan et al., 2005).

Correct Routing Discovery Guarantee: If there is a route in between the source node and the destination node, the secure routing protocol should be able to find the route and also able to check the correctness of the selected route (Karthigeyan et al., 2005).

Network Topology Confidentiality: If the attacker performs the information disclosure attack, it leads to discovering the network topology by the attacker node. If the attacker gets the network topology, it can also find the traffic pattern of the network. If the attacker finds some nodes that are used more in terms of network data traffic sending compared to other nodes, then the attacker can perform the denial of service (DoS) attacks on that node. So that the network can be jammed and the resources of the network can be wasted. Because of that, the confidentiality of the network is an important aspect to be added in the secure routing process (Karthigeyan et al., 2005; Karlsson et al., 2012).

Constancy Against Attacks: Deployed routing protocol must be able to self-heal to get back to its normal operating conditions after being affected by active or passive attackers. The routing protocol must be robust enough to survive the disruption of the network and resume at least its essential services even if the system is under attack (Karthigeyan et al., 2005).

2.2 Secure Routing Protocols for MANETs

Routing protocols in MANETs must fulfill the above-listed requirements in order to cope up with adverse network conditions and external attacks. Based on the characteristics of the routing process, routing protocols for MANETs are generally classified into reactive, proactive, and hybrid categories. Security can be added to the existing routing protocols considering their type and other fundamental requirements. One such classification is illustrated in Fig. 3.

Secure AD HOC On-Demand Distance Vector Protocol (SAODV): This protocol is an extension to AODV protocol. The working of SAODV involves the use of digital signatures for authentication purposes, while hashing is used for providing integrity to the routing messages. SAODV also addresses the issues of managing keys which is very important for a strong authentication mechanism. SAODV protocol uses cryptographic techniques and hash chaining. For every RREQ and RREP, a seed is generated and the hash field is set to its value and the max count of the hop is equaled to the value in the TTL field. The hash function is applied to the seed, max hop count times. This result is stored in the top hash field. Except for the hop count field, the node digitally signs all fields of the message of AODV header and has a field of SAODV extension header. Each intermediate node verifies the hop count with the difference of max hop count and hops count to the top has field. If not verified, the packet is dropped else the hash field is hashed once in the signature extension and then rebroadcasted to its neighbors. For sending a RERR message, the node generates a message and signs it using a digital signature. Only the destination sequence numbers are not hashed. Every neighbor that receives the RERR message and verifies the signature (Abusalah et al., 2008b).

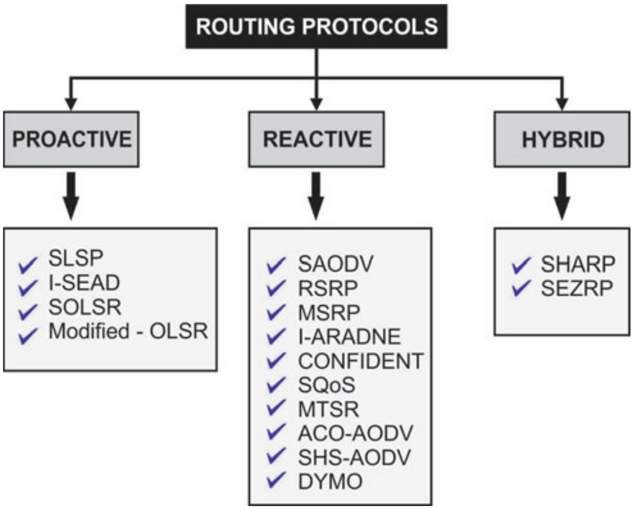


Fig. 3 Types of secure routing protocols

Robust Secure Routing Protocol (RSRP): RSRP is a secure routing protocol proposed to overcome the security concerns of a DSR reactive routing protocol. It is a lightweight and authentication-based protocol that can resist colluding attacks. Its robustness lies in the ability to quickly identifying malicious behavior and securing the network by dropping invalid/corrupted messages from attackers/suspicious nodes. RSRP protects the network from routing discovery and flooding attacks and also maintain the topology related information correctly, thus, preventing performance degradation due to attacks. In RSRP, source nodes and intermediate nodes can be authenticated by destination nodes. The source, as well as destination nodes, checks the correctness of the sequence of nodes in the node lists. The source node can also construct their own identities and broadcast the same to the other network nodes. The other network nodes can verify the identity of the source node but cannot reproduce it.

RSRP is a modified version of DSR protocol which includes additional features like efficient route discovery and maintenance, point-to-point, and MAC authentication. It also supports the broadcast authentication mechanism in which the sender node generates an identification message which can be verified by only the receiver node. RSRP can be customized for the required broadcasting mechanism to confirm the identity of the sender (Afzal et al., 2008).

Secure Routing Protocol for Mobile (MSRP): The MSRP protocol can be seen as the extension for providing security in the existing routing protocols, DSR, and ZRP especially. In MSRP, security provision is facilitated by the security association (SA) between two nodes—the source and the destination. With the help of a shared secret key, two control messages, route requests, and route reply are exchanged between the communicating parties to establish a secured connection.

MSRP mitigates the harmful effects of malicious behavior in providing correct connectivity information. The protocol guarantees that route replies that have been fabricated, compromised, or replayed would either be rejected or never reached the querying node back. In addition, the sensitivity of the protocol is safeguarded under various types of attacks that exploit the routing protocol itself. The protocol's sole requirement is that any two nodes that want to securely communicate can simply set up a priori shared secret to be used by their routing protocol components. In fact, there is no assumption about the intermediate nodes, which display unpredictable and destructive behavior. The scheme is stable in the presence of a variety of non-colluding nodes and offers timely and reliable routing information (Zhitang & Shudong, 2007). More pertinently, MSRP can be used across a broad spectrum of applications, without any specific constraints about the underlying credibility, network size, and participation. In addition, the protocol's validity is retained regardless of any permanent binding of nodes to IP addresses, an aspect of greater significance for open, diverse, and collaborative MANET environments (Zhitang & Shudong, 2007).

I-ARIADNE: Simple ARIADNE protocol only helps to provide the secure routing starting from a source node to the destination node but it does not provide security in between any two intermediate nodes. Therefore, to enhance the ARIADNE protocol and also provide the security for the intermediate nodes, an I-ARIADNE protocol is suggested. This protocol can detect any malicious participant node that attempts to modify the routing information. All the nodes that participate in a route trust the available routing-related information and use it again for another routing discovery phase. A source node computes the hash value h0 using its provided private key, and after that, all the network nodes participating in the route discovery process are authenticated by h0 which is calculated based on the hash function of the sender node. If the receiver wants to verify the routing message, then the sender also encrypts the h0 value using the shared key of the sender and receiver nodes. Intermediate network nodes can calculate the hash values and MAC values, and broadcast a routing message till the message reaches the receiver. As soon as the receiver receives the route request message, it verifies the hash value to check whether the sender is authenticated by decrypting the request packet using the shared key. The receiver signs the reply message using the secret key and then unicasts it on the path containing the list of nodes to be traversed. This way all the paths maintain the secret key (also known as the TESLA key). After sending the reply message, the receiver adds intermediate nodes on the route and the sender checks the authentication of the reply message by applying the shared key.

In I-ARIADNE, not only the sender and receiver node but all other nodes participating in the message transmission can also verify the correctness and validity of the established route. The source node unicasts a valid message and includes the sender value, receiver value, initial hashing value, list of nodes, and TESLA key value in the routing packet. Intermediate nodes use the hash chain to verify the MAC values using the TESLA key. I-ARIADNE provides improved security as well as better performance compared to ARIADNE (Lin et al., 2008).

CONFIDENT: Cooperation Of Nodes: Fairness In Dynamic Ad Hoc Networks (CONFIDANT) is a secured on-demand routing protocol, which secures communication networks by making the misbehaving nodes less important ones for the other nodes existing in the network. It aims to detect and isolate the misbehaving network nodes from the communication path such that they cannot harm the whole network or get the control packets for the routing process (Abusalah et al., 2008b). Protocol's trust relationship maintenance and route selection decisions are based on the observation of the network nodes, detecting malicious behavior, and trust vote reports generated for network nodes.

CONFIDANT consists of the mentioned components namely: monitor, reputation system, path manager, and trust manager. Every node in the network monitors the behavior of their next-hop neighbors. If a node detects some suspicious behavior by their neighbors, then that information is forwarded to the reputation system. The reputation system checks whether the event has occurred more than a predefined threshold. If it is higher than the threshold, then it is concluded as a malicious behavior of that particular node. These events are given some significant ratings based on their security requirements. If the threshold is bypassed, then the reputation system updates the intolerable rating to the path manager which deletes all the routes containing that particular node with the intolerable rating. It is then sent to the trust manager which sends an ALARM message which contains a type of protocol violation, number of observed occurrences, address of reporting node, whether the message was originated by the sender himself and the destination address. When the monitor receives this ALARM message, it passes it to the trust manager where the source of that message is found out. The disadvantage of CONFIDANT is that the distributed nature of the protocol leads to inconsistency problems related to reputation values (Abusalah et al., 2008b).

Securing Quality of Service Route Discovery (SQOS): This protocol is a secured protocol compared to one of the QoS routing discovery network protocols. SQoS protocol works based on the concept of symmetric cryptography. The protocol uses symmetric key cryptography which is always 3 to 4 times faster compared to the asymmetric key cryptography. This protocol is developed based on the hash chain method. If X is some random number, then the hash of X is calculated as Y = H(X); where H is a one-way hash function. The hash chain contains computed hash values like H(X), H (H(X)), and so on, by using the previously generated hash values for the next hash computation. The sender sends (n-1) th value to the receiver for the authentication purpose. For the next calculation, the sender sends the (n-2)th value to the receiver for the authentication purpose.

Furthermore, the MW chain also provides authentication with very low storage overhead. MW chain works basically on the one-time signature value, using the following sequence of operations: Each node selects the private key K that is used to generate the verification value key V and signature value S. Now, if the sender wants to send any message, then it sends the message using the value S. Only the network nodes that are communicated with the key V can read the decrypted packet. This way each of the messages can be signed with different values of S and verified using either the same or new value of V. MW works in a similar manner as the hash function except that the extra security property of signature S is added using key $Ki + 1$ that is used to generate the value Ki using the equation $Ki = f(s, m)$, but it cannot be used to get the value $Ki+1$.

As described above, SQoS replaces the hash chain with the MW chain because it provides security against the modification of the immutable fields of the requests. Other than that, SQoS also offers a computationally effective way to handle route requests flooding. Moreover, all the metrics initiators of the communication network nodes give the maximum and minimum required levels, hash chain length, and also a specification for executing the steps either linearly or in logarithmically (Abusalah et al., 2008b).

Multipath Trust-Based Secure Routing Protocol (MTSR): MTSR is a distributed protocol that is based on AODV and SAODV and can withstand almost all possible routing attacks such as discarding, Sybil, spoofing, jamming, flooding, rushing, and particularly wormhole attack. The trust value estimation follows the concept of gradually increasing yet rapidly declining, which involves no additional hardware, strict assumptions, and node position which specific time information.

In MTSR, generated hash values in the hash chain for the routing packets are always verified. One limitation of the protocol is that it cannot detect the attacks in which the hop count values remain the same or the hash values are missing. For each RREQ or RREP routing packets, each intermediate node in the route calculates the hash value and forwards it to the next node. Intermediate nodes also verify the previously generated values available in the hash chain and determine whether to increase the hop count. The selection of a route depends on the probability valued computed for each route.

If the intermediate node of the route drops all the messages (black hole) and/or selectively discarding the packets (gray hole), then the node's neighbors will reduce the trust value which is associated with it which might result in isolating that node to prevent any further attacks. Other attacks that are also prevented using this protocol are Sybil, wormhole attack, routing spoofing, and jamming attacks (Qiu et al., 2010).

ACO-AODV: This protocol follows a hybrid type of routing (Khanpara et al., 2010). ACO-AODV protocol is mainly used for dynamic clustering for a heterogeneous network to transmit data with the help of multicast routing between cluster heads (CH) and sink nodes. So, as to establish the route AODVR and Diffie–Hellman key exchange, algorithms are used to provide secure transmission of data. All the functionality of storing the public key is removed, and this way the overhead can be reduced. It uses a predictive methodology for casting the movement of the node and also proactively sends the source cluster details. If the CH is moved, it can be projected and a cluster reflection procedure is attained. The primary cluster formation is done using ACO clustering techniques. The assignment of CH is based on the weight values of the nodes and the least weighted node is chosen as CH. In case the node starts to interchange between clusters, then the source CH can forecast the mobility of the node and further can send the source details to the targeted CH. If the CH has the movement possible, then it can be projected and clusters reflection procedure can be achieved. This protocol is capable of creating a secure and safe environment for the data packet. Also, the protocol is efficient in terms of throughput, delivery of packets, packet loss, end to end delay, and energy consumption as well (Moudni et al., 2016).

SHS-AODV: The basic handshaking task performed by AODV to establish the network connection and communication can be attacked by malicious users. To overcome this, the sender node is made to generate the key pair with the use of the RSA algorithm, wherein one key is kept private while the other public key is made to be used by the destination node. This protocol uses reactive routing. While at the sender's side, the ECC algorithm is applied to encrypt the public key while the sensitive part is encrypted using the private key of the sender and then finally broadcasted as an RREQ packet. When the RREQ packet is received at the destination, a private key is used to decrypt the RREQ packet. It compares the public key in the RREQ packet, and if it matches then it sends the RREP packet by encrypting it using the public key of the sender. This protocol is capable of identifying a black hole attack, as the encrypted message is exchanged which can be adjusted by authenticating nodes. This reduces the chances of forgery attacks as fake packets are detected by source and destination nodes. This protocol is sensitive to the conditions which are delay sensitive also has a high-security fundamental (Rajput & Trivedi, 2014).

DYMO: This protocol uses a reactive routing method. DYMO creates less overhead in route table maintenance due to the use of path accumulation function (Nayyar, 2013). In this routing protocol, only the information which is necessary related to the source and destination is maintained while other protocols need to maintain all the fields of the record. The protocol involves two operations mainly, which are (1) route discovery and (2) route maintenance. Source initiates the broadcast of the RREQ packet, which includes a source address, destination address, sequence number, and other fields. After the RREQ packet is received, the intermediate node establishes a backward path to the source node along with appending its IP address to the RREQ messages. Here, the aim is to accumulate the path and reduce the number of RREQ message transmissions in further discovery of path. The route maintenance component includes two sub-components: (1) Route lifetime: It is extended in case of successful packet delivery and (2) Failure of link: Any broken link information is sent through RERR packet transmissions. The advantage of this protocol is that end to end delay is better compared to that of LAR protocol as DYMO avoids routing loops and obtains fresh information about the router. Hence, the risk of using stale information to cause an attack can be avoided. Also, in this protocol, the invalid routes are deleted, hence malicious nodes cannot use those routes to perform an attack. The only disadvantage of DYMO is the issue that arises in improving performance (Sreevidya & Nagaraja, 2018).

Secured Link State Routing Protocol (SLSP): This routing protocol uses proactive routing. SLSP is a secured routing scheme specially designed for proactive routing for mobile and ad hoc networks. It can be taken into use for standalone services as part of proactive link state routing. This can be also used for the hybrid framework as well, which can be further combined with other reactive and ad hoc protocols. The requirement for the implementation of this protocol is to have an asymmetrical key pair for each network instance (Abusalah et al., 2008b).

The implementation of this protocol involves the execution of three major steps, which are: (1) Distribution of public key: Its main task involves the broadcasting of the public keys. This broadcasting is done inside each zone with the use of a distributed key which is signed using the public key. (2) Discovering the neighbor: The node's information related to the link state is broadcasted regularly with the use of neighbor lookup protocol which is considered as an internal part of SLSP. In this case, each node dispatches its MAC address and its IP address of the existing network interface to its neighboring nodes by circulating NLP HELLO messages. (3) Updating of link state: Identification of packets is done through accessing its initiating node and also includes a 32-bit sequence number, which provides a lot of updation related to space. One of the major advantages of this protocol is that it provides protection against denial of service attacks. This is achieved by maintaining the priority ranking of the neighbor nodes. It is also capable of providing a secure proactive discovery of topology specifically for mobile and ad hoc networks. Hence, it also guarantees protection against individual malicious node attacks. The protocol also has some disadvantages that are it is vulnerable to colluding attackers. These attackers are capable of fabricating the non-existing links which exist between each other nodes and also dispatch this information to the neighbors.

I-SEAD: This protocol is also based on proactive routing. The functionality of routing is based on letting the neighbor nodes check how correct the hash value is and eventually reduce the overhead caused due to it in the routing. There are following steps involved in this protocol: (1) A request message is sent through the start node and also the node chooses a seed value randomly. (2) A list of values is computed by the start node in relation to the seed value so selected. (3) A MAC value is computed by the start node before the route request is sent. The MAC value is encrypted using the TESLA key so as to protect the hash value. (4) Each node then verifies the value received to them, after the given period of time is over (RPL, 2012). The use of this protocol is advantageous as it is responsible for securing the routing maintenance and improving the scalability. Also, it prevents the attacker from tampering the next-hop values or value of the destination field in route updates. The major drawback of this protocol is that it follows a very time-consuming process to secure the route. I-SEAD gives a better performance compared to the SEAD protocol in terms of scalability, mobility, and capability (Lin et al., 2008).

Secure Optimized Link State Routing (SOLSR): OLSR (non-secured) is a proactive routing protocol. OLSR control messages include two types of packets: HELLO and topology control. HELLO, messages are exchanged periodically among neighbor nodes, to get availability details of the neighbors and to know whether the neighbor is available or not for communication. The purpose of a topology control message is to share the topology information to the entire network. For secured OLSR (SOLSR), the created HELLO and topology control (TC) messages are sent to the neighbor nodes, and along with that, a timestamp is also generated. The timestamp is used for replay protection. Then, the signature is computed for authentication purposes. When a node receives a HELLO or TC message, the node waits for the corresponding signature message. When it receives the signature message, it is verified along with verification of time stamp, and the message is accordingly selected or rejected (Ahmad et al., 2017).

Modified OLSR: The protocol uses proactive routing. It uses an updated multipoint relays (MPR) procedure to detect and mitigate the node isolation attack. This mechanism is also helpful in the prevention of any malicious or stale or false nodes from giving wrong information about true nodes that is willing to become MPR (Srivastava et al., 2013). There are two new messages introduced along with HELLO and TC messages, which are VOTEFOR and VOTERPL. The process involves sending of VOTEFOR message to a node's first-hop neighbor and further it sends to the second hop neighbor. When the node receives the reply to these messages, then the VOTERPL message gets generated which is sent back to the sender through the one-hop neighbor. This information is recorded in the routing table.

Modified OLSR is used mainly for the detection and mitigation of the node isolation attack. But the drawback of this protocol is that it can only be used for OLSR which needs to be expanded to other protocols as well. It makes the network complicated as new nodes keep on adding into the network. This results in the selection of less number of nodes as MPR increases the packet delivery ratio, average TC size, PDR, and energy consumption (Srivastava et al., 2013).

Sharp Hybrid Adaptive Routing Protocol (SHARP): It makes the use of both proactive and reactive routing. There are proactive zones established around the hubs. It controls the number of hubs by hub specific zone territory in a proactive zone. A reactive mechanism for a destination hub is used if, in a proactive zone, a hub is not present and then also to set up a route to that hub. In a proactive zone, a proactive mechanism is used. If some particular nodes are frequently contacted or searched for then they are grouped in a proactive zone. Once the group is established at any hub at the proactive zone, these proactive zones gather packets and forward them to the destination (Remya & Lakshmi, 2015).

SEZRP: SEZRP is a hybrid protocol. The authentication technique used in this protocol is hashed message authentication code to provide integrity. The key distribution technique is also used to minimize the overhead which is caused due to the distribution of keys during the execution. This protocol is a security-enhanced zone-based routing protocol, which uses point-to-point authentication because it can authenticate various types of routing control packets. In case, the attacker changes any values in the field, the protocol is able to detect the same easily. This protocol is one of the successful MANET protocols as it provides the integrity of the routing packets in ZRP. SEZRP can prevent a variety of attacks such as black hole attacks, modification of routing information attacks, and impersonation attacks. In the presence of malicious nodes, the performance of this protocol turns out to be better than ZRP. But as this comprises so many tasks, the performance of this protocol is no way different than the ZRP specifically in the absence of malicious node (Srivastava et al., 2014).

Highly Secure Geographic Routing (HSECGR) (Boulaiche & Bouallouche-Medjkoune, 2017): It is assumed in this approach that every node in the network knows its position, its neighbor's location, and the destination's location. Location information is obtained by GPS. The neighbor's position is obtained by position beacon messages. One more assumption is that a secret key is shared between pairs of source and destination which is distributed by a key distribution center. When a source sends a message toward the destination, it keeps a packet's copy for comparison with the acknowledgment packets. Also, source nodes initiate a timer, if the destination acknowledgment is not received until the timeout, the source node considers the packet as dropped. Each intermediate node compares the received MAC value to the computed MAC value. The computation of the MAC value is done using the packet header and the shared key. If authenticated, an acknowledgment packet is sent by an intermediate node to the source node.

Secure Route Discovery for Dynamic Source Routing (SRDP) (Kim & Tsudik, 2009): SRDP protocol works over the base protocol DSR. To secure the DSR protocol, the route discovery phase is secured in this technique. Two things are assured of doing this, out of which one is avoiding the feedback loop. A feedback loop is defined as a list of connected legitimate nodes in-between two compromised nodes of attacker nodes. So, each intermediate node included in the source route must be authentic. Secondly, the source should be able to verify all the intermediate nodes and the destination node. Assumptions made in SRDP are that both the source and the destination are authentic and nodes are not aware of their immediate neighbors. Cryptographic techniques used by this protocol are shared key MACs and public key signatures. An authentication tag is used by each node to convince the source node that the node belongs to the source route and is legitimate. The source node needs to definitively receive each authentication tag as a part of the RREP flag. MACs are preferable as compared to the encryption techniques for authentication purposes. For source node authentication, RSA is used.

Reputation-Based Internet Protocol Security (RIPSEC) (Lacey et al., 2012): Before the network is established, or the nodes are deployed, PKI certificates are distributed to all the nodes. These certificates are sued to establish a security association and also to sign and encrypt data. Every node pair has two pairs of SA one for authentication and another for encryption. The transport layer consists of IPSec to provide transmission security. No intermediate node can decrypt the data because the key is shared only with the source and the destination. A summary of the secured MANET routing protocols is presented in Table 2.

3 Application of MANET Protocols in the IoT Domain

Growth of IoT devices and control systems is increasing day-by-day and as per the IoT analytics of 2018 (Lueth, 2018), there will be approximately 22 billion IoT connected devices until 2025. In IoT systems, the sensory devices are connected in the wired or wireless manner to communicate, process, and make intelligent decisions based on the processing. However, there are many applications of IoT where the use of wireless network connection is essential and ad hoc networks become the best choice due to resource constraints and the necessity of continuous communication. In such scenarios, existing MANET-based routing techniques can be applied directly in the IoT device communications. As security is one of the major concerns in ad hoc networks, it becomes essential to use routing protocols that are robust against a variety of network attacks so that the required network services can be provided even under adverse situations (Khanpara & Trivedi, 2018). The previous section describes a wide range of secured MANET routing protocols that can be used to facilitate secured communication in the MANET-based IoT environment. The protocols discussed in the previous section use various techniques such as cryptography, hashing, and other modifications in the conventional routing methods to make them more secure and robust against a variety of attacks and misbehaviors (Alam vided even under adverse Rababah, 2019).

Based on (Alam, 2019a), initially, IoT used to connect the devices with the World Wide Web (WWW) since 2008. After that, IoT has shifted its technology from data-based to the operation-based technology and also switched data transmission from man to machine to machine to machine by upgrading from IPv4 to IPv6 (Alam, 2019b). With the growing technology of machine to machine (M2M) interaction, a number of innovative communication techniques have been proposed for the IoT environment. These techniques are generally evaluated based on complexity, performance, cost, and security parameters. There is always a trade-off between the performance and security which also directly affects the complexity of the design and the overall cost of implementation. Therefore, there are very few communication techniques available so far that can balance all the assessment parameters and offer a good level of performance in the given IoT scenarios. This is the main reason for researchers to use routing protocols of underlying networks in the IoT domain to propose cost-effective, efficient, and secured mechanisms for communication without investing the efforts in designing the completely new IoT-specific routing mechanisms (Alam & Benaida, 2019).

MANET-IoT system technology is based on three major technologies. The ubiquitous computation supports IoT physical devices for data transfer and uses secured MANET routing protocols or proposes additional mechanisms to secure the ad hoc network routing. As IPv4 is not enough and capable of transferring the data from machine to machine IoT systems, IPv6 is used to connect billions of devices and communicating parties to transfer the data. IPv6 also needs to be highly secured as there are billions of IoT devices connected around the world and confidentiality/privacy is a major concern. To deal with the mobility in sensor interconnected devices, MANET-IoT systems use omnipresent computations. This technique needs to improve whenever smart devices' advancements take place and/or multi-sensor structures improve in terms of storage, calculation, evaluation, and reduction in size or reduced power consumption (Alam, 2015).

4 Open Challenges and Future Directions

IoT and MANETs both technologies are in growing phase so that there are many challenges in the implementation of the same. In this chapter, we focused on the security and connectivity of IoT devices and their communication compatibility with the MANET protocols. As security is one of the most important features in the success of the IoT systems and MANETs provide security which is highly accepted and appreciated by the IETF group, we have proposed to use MANET routing in IoT environments. A survey on secured routing mechanisms for MANETs in IoT domains is presented along with their advantages and limitations. Based on the analysis of these mechanisms, it has been found that there are still open challenges in the usage of secured MANET protocols with IoT system devices such as—establishing secure routes, self-robustness, identifying malicious nodes/actions, computationally inexpensive processes, and confidentiality of locations (Sehgal et al., 2020; Singh et al., 2020b).

Moreover, identifying the malicious nodes of the network and rejecting it appropriately such that no other node uses it as a packet sending hop is one of the highly challenging research questions currently in MANET routing protocols.

Table 2 Summary of the secured MANET routing protocols listed above is presented

Name	Key features	Advantages	Limitations	Attacks dealt with
SAODV (Abusalah et al. 2008b)	One-way encryption (hashing)	Securing AODV packet's changeable field to protect the network from malicious packet	Malicious nodes can collude to send the same/new random number	Black hole and malicious packet tempering
RSRP (Afzal et al. 2008)	Destination node authenticates source and intermediate nodes	Uses broadcasting authenticated protocol to prevent from colluding attacks; robust	Point-to-point authentication security is not feasible	Routing discovery process disruption and flooding attacks
MSRP (Zhitang & Shudong 2007)	Exchanges message secret key between source and destination	Request and reply node never collude	Pre-assumed that intermediate nodes are non-colluded	Security against the false requests and false replies
I-ARIADNE (Lin et al. 2008)	Authenticate message using secret (TESLA) key	Detects any malicious node in the network	Higher computation cost	Denial of service attacks
CONFIDENT (Abusalah et al. 2008b)	Detects and isolates the misbehaving network nodes from the communication	Routing is based on nodes reputation (feedback from other nodes)	The distributed mechanism developed leads to many different inconsistencies to the reputation value	Prevents from sending a message to outside the network
SQoS (Abusalah et al. 2008b)	Symmetric cryptography	Packet transfer is faster, less delay, and higher bandwidth	Less secure than other asymmetric cryptography protocols	Attacks targeting QoS, the modification of the immutable fields of route requests
MTSR (Qiu et al. 2010)	Hash chain is used for message routing from source to destination	Works for unicasting and broadcasting messages in the network	Cannot detect the attack of keeping the same values of hop counts and also the missing hash operations	Sybil, wormhole attacks, routing spoofing, and jamming attacks
ACO-AODV (Moudni et al. 2016)	AODVR and Diffie–Hellman key exchange algorithm are used to provide secure transmission of data	Efficient in terms of throughput, delivery of packets, packet loss, end to end delay, and energy consumption	Protocol's proposed algorithm is not optimized	Packet modifications
SHS-AODV (Rajput & Trivedi 2014)	RSA + ECC algorithm is used	High-security fundamentals	Communication delay sensitive	Forgery and black hole attacks
DYMO (Sreevidya & Nagaraja 2018)	Only the information which is necessary related to source and destination is maintained using accumulation function	The protocol creates less overhead in path link table maintenance	Low performance	Stale information attacks
SLSP (Abusalah et al. 2008b)	Use public key distribution, link state update, and neighboring discovery	Works as a standalone system for the proactive route scheme and/or can be one of the hybrid routing combined with the reactive routing	Requires the existing asymmetric pair of keys for each network interface	Denial of service attacks
I-SEAD (Lin et al. 2008)	A hash key value is used to compute the packet validation	Only neighbor nodes compute hash values to verify the node's trustworthiness	Overhead of periodically counting hash new value updates	Routing spoofing and black hole attacks
SOLSR (Ahmad et al. 2017)	HELLO messages are exchanged periodically among neighbor nodes to get availability details of the neighbors	The entire network reflects the updated network topology	Overhead of sending topology information periodically to the entire network	Security against the false requests and false replies

(continued)

Table 2 (continued)

Name	Key features	Advantages	Limitations	Attacks dealt with
Modified OLSR (Srivastava et al. 2013)	Sends HELLO messages and expects replies hop-by-hop	The protocol can detect and mitigate the node isolation attack	Adding new nodes in the network makes the network more complicated	Node isolation attacks
SHARP (Remya & Lakshmi 2015)	The hybrid mechanism is used based on the reactive or proactive zone, and the zoning mechanism can be set	Controls the number of hubs by hub specific zone territory in a proactive zone	Low performance	Route spoofing
SEZRP (Srivastava et al. 2014)	Point-to-point authentication using the hash key	Key distribution technique is used to minimize the overhead of hashing functionality	Helpful only in zone-based security provision	Black hole, impersonation, and modification of routing information attacks
HSecGR (Boulaiche & Bouallouche-Medjkoune 2017)	Acknowledgment and timer-based packet transmission from source to destination	Nodes attached with GPS, know own, neighbors' and destination's location in the network	Assumed secret key distribution is secured	Routing attacks and location-based compromise attacks
SRDP (Kim & Tsudik 2009)	Cryptographic and encryption techniques used for node authentication	Source node authentication, only legitimate nodes in the established routes	Overhead of authenticating each node in the route	Black hole attack and wormhole attack
RIPSec (Lacey et al. 2012)	Encryption and signed certificate-based data transmission	No intermediate node can decrypt the data	Third party for issuing certificates	Security against the false request and false reply attacks; impersonation

There are different trust models for MANET routing protocols that are proposed to use in the IoT system devices which provides enhanced security and high network availability based on the given requirements. Even after fulfilling all the possible requirements of IoT system connectivity, there are some open challenging research questions. Not only in the IoT systems, but security is also one of the most challenging issues for many other applications where devices and machines are connected via the Internet to transfer data. In such systems, routing in a secured manner is the critical problem that must be solved considering the requirements of the given system. One of the most emerging systems amongst them is robotic technology, where the security of communication and other processes plays a vital role. Due to the requirements of such systems, MANET routing methods are quite suitable to use in the robotics domain (Mahapatra et al., 2019).

A well-known MANET-based automated convention protocol PD-ROBO (Rath & Pattanayak, 2019) supports the committed intrusion detection system (IDS) structure that is useful in utilizing the portable operator method and defends the system against replay assault attacks in mechanical-based MANETs. The PD-ROBO MANET protocol's framework is designed based on the secure and robust MANET protocol and Power and Delay Optimized AODV Protocol (PRO-AODV). PD-ROBO protocol also imports striking features from MANETs' protocols such as energy efficiency, load balancing, and controlled delay in processing. Furthermore, it is also implemented with a prospect of efficient communication between the robots in the robot-based mobile ad hoc networks. For this, it works on different parameters such as network scalability and improvement of the network lifetime to prolong the communication period among the robots (Rath & Pattanayak, 2019). Though researchers have proposed MANET-based routing protocols for IoT and robotics domains, a good amount of research is still needed around network protocol scalability, energy efficiency, reliability, security, and mobility support leading to the effective design, development, and deployment of robotic systems to improve the overall performance. With the rapid growth in the IoT technologies, new and emerging MANET-connected systems will come up with an altogether new set of security and connectivity challenges and risks that requires new and innovative solutions from the researchers.

References

Abusalah, L., Khokhar, A., & Guizani, M. (2008a). A survey of secure mobile ad hoc routing protocols. *IEEE Communications Surveys & Tutorials, 10*(4), 78–93.

Abusalah, L, Khokhar, A., & Guizani, M. (2008b). A survey of secure mobile Ad Hoc routing protocols. In *IEEE Communications Surveys & Tutorials* (Vol. 10, Issue No. 4, pp. 78–93), Fourth Quarter. https://doi.org/10.1109/surv.2008.080407.

Afzal, S. R., Biswas, S., Koh, J., Raza, T., Lee, G., & Kim, D. (2008). RSRP: a robust secure routing protocol for mobile ad hoc networks. In *2008 IEEE Wireless Communications and Networking Conference*, Las Vegas, NV (pp. 2313–2318). 10.1109/WCNC.2008.408.

Ahmad, M., Chen, Q., Najam-Ul-Islam, M., Iqbal, M. A., & Hussain, S. (2017). On the secure optimized link state routing (SOLSR) protocol for MANETs. In *2017 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*, Nanjing.

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications, 66,* 198–213.

Alam, T., & Aljohanim M. (2015). Design and implementation of an Ad Hoc Network among Android smart devices. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1322–1327). IEEE. https://doi.org/10.1109/ICGCIoT.2015.7380671.

Alam, T. (2019a). IoT-Fog: A communication framework using blockchain in the Internet of Things. *International Journal of Recent Technology and Engineering (IJRTE), 7*(6).

Alam, T. (2019b). Blockchain and its role in the Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5*(1), 151–157. https://doi.org/10.32628/CSEIT195137.

Alam, T., & Benaida, M. (2019). The role of cloud-MANET framework in the Internet of Things (IoT). *International Journal of Online Engineering (iJOE), 14*(12), 97–111. https://doi.org/10.3991/ijoe.v14i12.8338.

Alam, T., & Rababah, B. (2019). Convergence of MANET in communication among smart devices in IoT. *International Journal of Wireless and Microwave Technologies (IJWMT), 9*(2), 1–10. https://doi.org/10.5815/ijwmt.2019.02.01.

Boulaiche, M., & Bouallouche-Medjkoune, L. (2017). Hsecgr: Highly secure geographic routing. *Journal of Network and Computer Applications, 80,* 189–199.

Bruzgiene, R., Narbutaite, L., & Adomkus, T. (2017). MANET network in Internet of Things system. In J. H. Ortiz & A. P. de la Cruz (Eds.), *Ad Hoc networks*. Rijeka: InTech. https://doi.org/10.5772/66408.

Deepika, D., & Anand, N. (2013). Complete scenario of routing protocols, security leaks and attacks in MANETs. *Journal Proceedings of the IJARCSEE, 3*(10).

Dhiman, D., & Nayyar, A. (2013). Complete scenario of routing protocols security leaks and attacks in MANETs. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(10).

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Karlsson, J., Dooley, L., & Pulkkis, G. (2012). Routing security in mobile ad-hoc networks. *Issues in Informing Science and Information Technology, 9,* 369–383.

Karlsson, J., Dooley, L. S., & Pulkkis, G. (2018, August). Secure routing for MANET connected Internet of Things systems. In *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 114–119). IEEE.

Karthigeyan, I., Manoj, B. S., & Murthy, C. S. R. (2005). A distributed laxity-based priority scheduling scheme for time-sensitive traffic in mobile ad hoc networks. *Ad Hoc Networks, 3*(1), 27–50.

Khanpara, P. (2014). A review on fuzzy logic based routing in ad hoc networks. *International Journal of Advanced Research in Engineering and Technology, 5*(5), 75–81.

Khanpara, P., & Lavingia, K. (2020). Energy conservation in multimedia big data computing and the Internet of Things—A challenge. In *Multimedia Big Data Computing for IoT Applications* (pp. 37–57). Singapore: Springer.

Khanpara, P., & Trivedi, B. (2008). Survivability in MANETs. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 7*(1).

Khanpara, P., & Trivedi, B. (2017). Security in mobile ad hoc networks. In *Proceedings of International Conference on Communication and Networks* (pp. 501–511). Singapore: Springer.

Khanpara, P., & Trivedi, B. (2018). Survivability in MANETs. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 7*(1).

Khanpara, P., Valiveti, S., & Kotecha, K. (2010). Routing in ad hoc network using ant colony optimization. In *International Conference on Future Generation Communication and Networking* (pp. 393–404). Berlin, Heidelberg: Springer.

Kim, J., & Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs. *Ad Hoc Networks, 7*(6), 1097–1109.

Lacey, T. H., Mills, R. F., Mullins, B. E., Raines, R. A., Oxley, M. E., & Rogers, S. K. (2012). RIPsec—Using reputation-based multilayer security to protect MANETs. *Computers & Security, 31(*1 (2012): 122–136.

Lin, C., Lai, W., Huang, Y., & Chou, M. (2008). Secure routing protocol with malicious nodes detection for ad hoc networks. In *22nd International Conference on Advanced Information Networking and Applications—Workshops (Aina Workshops 2008)*, Okinawa (pp. 1272–1277). https://doi.org/10.1109/waina.2008.47.

Lueth, K. L. (2018). State of the IoT 2018: Number of IoT devices now at 7B–market accelerating, 2018. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (visited on 03/04/2019).

Mahapatra, B., Patnaik, S., & Nayyar, A. (2019). Effect of multiple-agent deployment in MANET. *Recent Patents on Computer Science, 12*(3), 180–190.

Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2016). Secure routing protocols for mobile ad hoc networks. In *2016 International Conference on Information Technology for Organizations Development (IT4OD)* (pp. 17). IEEE.

Nayyar, A. (2012, January). Simulation based evaluation of reactive routing protocol for MANET. In *2012 Second International Conference on Advanced Computing & Communication Technologies* (pp. 561–568). IEEE.

Nayyar, A. (2013). Enhanced anomaly detection IDS-based scheme for dynamic MANET on-demand (DYMO) routing protocol for MANETS. *International Journal of Computer Science and Mobile Computing, 2*(4), 384–390.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 217–243). Academic.

Perkins, C. E. (2001, January). Ad hoc networking. Reading: Addison-Wesley.

Qiu, X., Liu, J., & Sangi, A. R. (2010). MTSR: Wormhole attack resistant secure routing for Ad hoc network. In *2010 IEEE Youth Conference on Information, Computing and Telecommunications*, Beijing (pp. 419–422). https://doi.org/10.1109/ycict.2010.5713134.

Rajput, S. S., & Trivedi, M.C. (2014). Securing zone routing protocol in manet using authentication technique. In *2014 International Conference on Computational Intelligence and Communication Networks* (pp. 872–877). IEEE.

Rath, M., & Pattanayak, B. K. (2019, January 1). Security protocol with ids framework using mobile agent in robotic MANET. *International Journal of Information Security and Privacy (IJISP), 13*(1), 46–58.

Remya, S., & Lakshmi, K. S. (2015). SHARP: Secured hierarchical anonymous routing protocol for MANETs. In *2015 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, 2015 (pp. 1–6). https://doi.org/10.1109/iccci.2015.7218121.

RPL. (2012). IPv6 Routing Protocol for Low-Power and Lossy Networks, Request for Comments (RFC) 6550, IETF. http://tools.ietf.org/html/rfc6550.

Sachs, G. (2014). The internet of things: Making sense of the next mega-trend. Technical report, Goldman Sachs.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Shah, M., & Khanpara, P. (2019). Survey of techniques used for tolerance of flooding attacks in DTN. In *Information and Communication Technology for Intelligent Systems* (pp. 599–607). Singapore: Springer.

Singh, U. (2011). Secure routing protocol in mobile ad hoc networks—A survey and taxonomy. *International Journal of Reviews in Computing, 7*(2), 9–17. http://www.ijric.org/volumes/Vol7/Vol7No2.pdf.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of Things: From hype to reality. *An Industrial IoT Approach for Pharmaceutical Industry Growth, 2,* 191.

Singh, S., & Kumar, D. (2020). Perceptions of security and privacy in Internet of Things. In *2020 International Conference on Inventive Computation Technologies (ICICT)* 2020 February 26, 2020 (pp. 810–813). IEEE.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020b). Internet of Things in pharma industry: possibilities and challenges. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 195–216). Academic.

Sreevidya, C, & Nagaraja, G. S. (2018). Secure multicast routing for wireless sensor networks using ACO-AODV with dhke cryptosystem. In: *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 733–737). IEEE.

Srivastava, A., Kumar, D., & Gupta, S. C. (2013). Geographic and reactive routing protocols for manet. In *2013 European Modelling Symposium* (pp. 590–594). IEEE.

Srivastava, A., Kumar, D., & Gupta, S. C. (2014). Modelling mobility in emergency scenario for manet applications. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)* (pp. 1–6). IEEE.

Tanwar, S. (2020). Fog data analytics for IoT applications—next generation process model with state-of-the-art technologies. *Studies in Big Data, 76,* 1–497. (Springer International Publishing).

Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Request for Comments (RFC) 4944, IETF, 2007. http://tools.ietf.org/html/rfc4944.

Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless network security 2007* (pp. 103–135). Boston, MA: Springer.

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 Ninth International Conference on Computational intElligence and Security* December 14, 2013 (pp. 663–667). IEEE.

Zhitang, L., & Shudong, S. (2007). A secure routing protocol for mobile ad hoc networks. In *6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)*, Melbourne, Qld. (pp. 153–157). https://doi.org/10.1109/icis.2007.43.

IoT for Smart Automation and Robot

Ashish Tripathi, Anand Bhushan Pandey, Arun Kumar Singh,
Pardeep Malik, Krishna Kant Singh, and Prem Chand Vashist

Abstract

The technology, which is behind this drastically changing world, is the Internet of things (IoT) and Internet of things connected devices. These devices are capable of communicating over the Internet by using various protocols designed for wireless networks. In recent years, IoT devices have flooded the market, and their services to the society and the world infrastructure are becoming vital. The growing demand for automation has accelerated the deployment of IoT devices across the world. Not only the intelligent IoT devices and sensors but the robots also have become the backbone of smart automation systems such as home automation, industrial automation, and city automation (smart cities). The increasing number of these smart devices and growing infrastructure is creating security and privacy challenges, but at the same time, a number of leading companies have extended their support to curb the threat that may be fatal if not taken seriously. Startups have also started working in fields like healthcare, transportation, and delivery of goods via IoT devices across smart cities. Monitoring of streetlights, air quality, noise and traffic of a city, security, and optimal use of home appliances in a home and development of innovative technologies and increasing the production in an industry are some of the IoT and robotic services that the world is already exploiting. This chapter discusses the importance of intelligent IoT devices and robotics today and in future in the domains like home automation, industrial automation, and city automation.

Keywords

Robotics • Internet of things (IoT) • Internet of robotic things (IoRT) • Artificial intelligence • Smart automation • Smart cities • Smart homes

1 Introduction

The Internet of Things (IoT) is one of the growing technologies that use the Internet to establish a connection among various IoT devices. IoT devices manage tasks like system activation, action specifications, communication, security, and detection. IoT devices include devices for a remote dashboard, for control, for servers, for routing or bridge devices, and sensors. These IoT devices are equipped with advanced features to communicate over the Internet via some wireless protocols. These devices can also be controlled and managed remotely as per requirement without the need for physical intervention. In recent studies, the rapid growth of IoT concepts has been encountered in various domains especially in the field of smart automation and robotics. These fields are using the inherent features of IoT to gain the desired progress and advancement in their work. In recent times, IoT has started a new era in the field of automation especially, in industrial automation, home automation, and developing smart cities. In industrial automation, IoT provides new solutions to industrial problems through the creation of innovative technologies, increasing production, and operations. In the recent survey of Gartner, it is predicted that by 2020, near about 21 billion IoT-enabled smart devices will be required all over the world, and during this time frame, the overall market growth will reach up to $3.7 trillion (Gartner, & McKinsey). These devices will be required in home automation, smart cities,

A. Tripathi (✉) · A. B. Pandey · A. K. Singh · P. C. Vashist
Department of IT, G. L. Bajaj Institute of Technology and Management, Greater Noida, India
e-mail: ashish.mnnit44@gmail.com

K. K. Singh
Department of Computer Science & Engineering,Faculty of Engineering & Technology, Jain (Deemed-to-be University), Bengaluru, India
e-mail: krishnaiitr2011@gmail.com

P. Malik
Department of Computer Science and Applications, DCRUST, Murthal, India

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_13

and other activities. This is posing a number of challenges and hence the responsibilities on the telecommunication leaders like creating new communication protocols, providing large address spaces (IPv6), creating standard but flexible architecture, and developing new devices that support IoT and increase privacy and security in IoT technology. Therefore, various companies are coming to this field as IoT service providers to provide the IoT-enabled devices.

As per the report of The Wall Street Journal, Google has acquired Nest Labs Inc. in 2014 in $3.2 billion, which specially deals in making smart thermostats and smoke alarms for homes (The Wall Street Journal). In this continuation, in 2015, another technical giant, Apple presented its first smartwatch in the market (Smartwatch). In recent years, many startups have been initiated in different domains such as health care, transportation, and consumer goods to ease of working through smart devices. In the development of smart cities, many projects have been initiated worldwide. This involves different activities such as adjusting the brightness of the LED streetlights, which depends on the distance of pedestrians from the LED. These lights are also equipped with other functionalities such as a Wi-Fi network to facilitate Internet access and the measurement of air quality, noise, traffic, and crowed. Likewise, the same effort has been seen in home automation. Home automation is also referred to as a smart home. Different facilities can be provided by home automation to the homeowners (Jose & Malekian, 2015). These facilities may include reduced energy consumption, optimized use of water, home security, effective use of home appliances, and comfort to the owner of the house. This becomes possible by controlling smart devices through a smartphone or any other networked device. A new concept, The Internet of Robotic Things (IoRT), has been given by the communities of IoT and robotics. The working concept of both things is different. To handle any specific task, IoT devices are specially designed to work, while robots generally first observe any unexpected or expected conditions and then react accordingly. A concept has been progressing very rapidly since 2016 based on the joint effort of the communities of IoT and robotics. This joint effort has been named as the Internet of Robotic Things (IoRT). Based on the recent study, it has been predicted that the market capitalization of IoRT will reach near to $21.44 billion by 2022 (Robotics & The Cloud). In IoRT, the robots are treated as intelligent devices with inherent sensing and monitoring capabilities to observe and take necessary action for the events occurring around them. This chapter has a discussion on the significance, role, and future of IoT in smart automation especially in-home automation, industrial automation and development of the smart cities, and robotics.

2 Past, Present, and Future of IoT

In 1912, first telemetry system which used telephone lines to monitor power plant data was developed in Chicago. The telemetry system got enhanced, and as a result, in the 1930s, a device named radiosonde was used for monitoring weather conditions (Munirathinam, 2020). With the launch of Sputnik in 1957 by the Soviet Union, a plate form for today's satellite communication was created (Holtorf & Piccini, 2009). In the 1980s, machine-to-machine communication began with wired connections in factories and home security systems which started using wireless connections in the 1990s (Sauter, 2010). In 1995, the first cellular module for a machine-to-machine communications was introduced by Siemens.

Today Google, Apple, and Cisco, the major ICT players take significant business decisions so as to make their position in the IoT landscape (Vermesan & Friess, 2013). The core business focus for telecom operators is machine-to-machine communication and hence the Internet of Things which has shown significant growth in the number of connected devices. Research and innovations in a variety of fields like embedded systems, network technologies, cyber systems, operating platforms, and semantic interoperability are being promoted as a result a number of components are available which the market can exploit (Tripathi et al., 2020; Singh et al., 2020a). The future of IoT is with other technologies like cloud computing, big data, semantic technologies, and robotics.

In future, the Web platform of smart environments and connected devices would be integrated with the Internet of things today to make a smart Web of everything to support the changes in the society and the growth in the economy.

3 IoT Architecture

Every IoT system has its unique architecture as per its applicability. But the foundation and all other activities such as gathering, transmitting, and processing of data are roughly similar in all architectures. IoT architecture consists of things (objects) such as sensors, actuators, and computing devices that are connected through standard wireless IoT protocols (Ren et al., 2017). Then, the objects are used to gather information from the environment around them and then transfer to the IoT gateways. Such collected unprocessed data is prepared for the analysis purposes after converting it into a digital stream, filtering, and preprocessing the data (Dubey et al., 2020; Sehgal et al., 2020). After that, the analysis of data starts through the latest technologies such as machine learning, deep learning, and visualization. Such processed and analyzed data are then transferred for storage in data centers. The data centers may be cloud-based or on local premises. As the number of IoT devices will be in billions and trillions in coming future and as the nature of these devices is heterogeneous, the IoT technology will require a flexible architecture (Gubbi et al., 2013; Padikkapparambil et al., 2020; Singh et al., 2020b). Three layers named as perception layer, network layer, and application layers were the part of most of the initial three-layered models given, while recent frameworks are having a five-layered architecture as shown in Fig. 1.

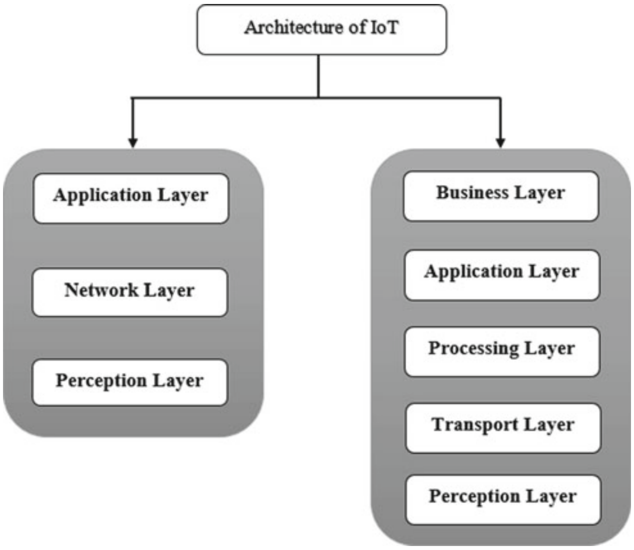


Fig. 1 Architecture of IoT

3.1 Three-Layer Architecture

It is the basic architecture of IoT as shown in Fig. 2. In the early phase of the IoT technology, this three-layer architecture was introduced. The details of theses layers are as follows.

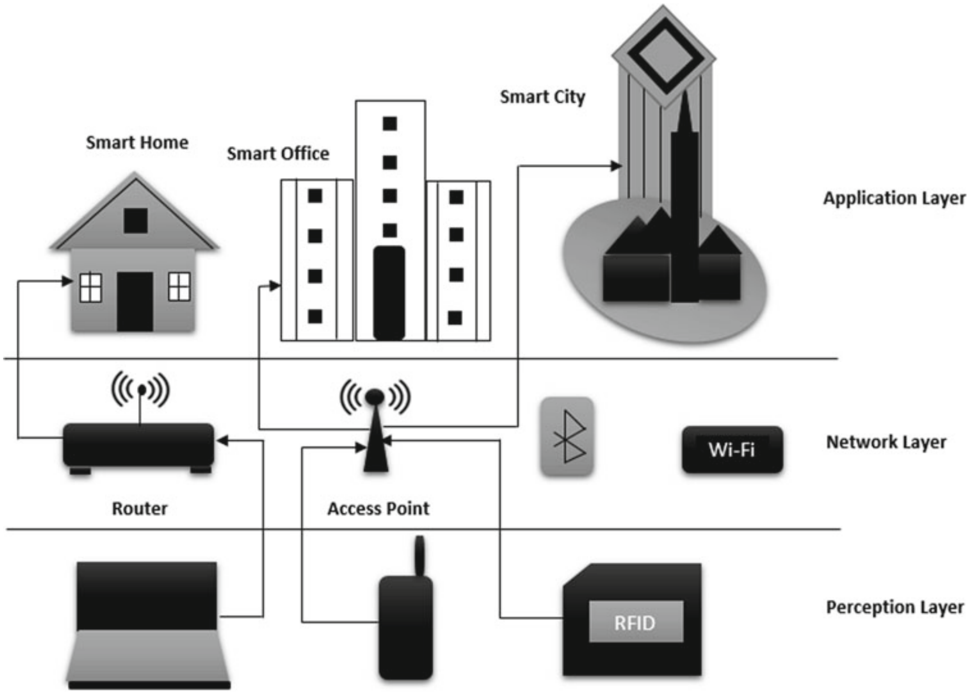
3.1.1 Perception Layer

It is the physical layer that deals with sensors and other physical devices to collect the environmental data that may vary as per the usability of the application for which it is applied. The devices of this layer identify different smart objects and collect data from those objects for further processing (Mashal et al., 2015).

3.1.2 Network Layer

This layer connects the IoT objects such as smart physical devices, servers, network devices, and networks to each other for transmitting and processing the data received from different sensors. This layer is also referred to as a transmission layer (Mashal et al., 2015). The medium of transmission can either be wired or wireless as per the requirement of the network. This layer is highly sensitive as per the attackers' point of view. Ensuring the integrity and

Fig. 2 Three-layer architecture of IoT



authentication of data is a significant aspect of this layer (Said & Masud, 2013).

3.1.3 Application Layer

The application layer is liable for delivering the services to the end-users. These services are application specific that uses an interface between the network and IoT devices for the smooth delivery of the services. This layer is responsible for providing services to various IoT applications, such as smart transportation systems, smart healthcare systems, smart homes, smart cities, and many more. For each application, the delivered services may vary based on the collection of data from sensors (Said & Masud, 2013). The application layer is executed with the help of a specific software application that is known as a Web browser. The Web browser is responsible for running various protocols of the application layer. These protocols include simple mail transfer protocol (SMTP), hypertext transfer protocol (HTTP), hypertext transfer protocol secure (HTTPS), and file transfer protocol (FTP) (Wu et al., 2010).

3.2 Five-Layer Architecture

We have discussed three-layer architecture in Sect. 3.1, which is the basic architecture of the IoT. This architecture tells about the key concepts of the IoT. But, some other significant parts of the IoT architecture are required to be discussed for ensuring the applicability of IoT in various applications. In the literature, much other layered architecture has been proposed. Five-layer architecture is one of them, which includes two additional layers, i.e., business and processing layers. The five layers include business, application, processing, transport, and perception layers. Perception and application layers are already discussed in the three-layer architecture. The remaining three-layers are discussed as follows.

3.2.1 Business Layer

The business layer is responsible for managing the complete IoT system. This layer deals with controlling and managing applications, maintaining the privacy of users, and profit and business models of IoT. It has also a significant role in the creation and storage of information (Zhong et al., 2015). This layer is an easy target for the attackers to misuse the business logic. Business logic attack and zero-day attack are the two common security problems of this layer. The business logic attack occurred due to the common programming flaws. The business logic attack includes stealing and managing the information during the information exchange between the user and the database of application software, while the zero-day attack occurs due to security holes that includes controlling the user's role without taking his consent.

3.2.2 Processing Layer

This layer is also called the middleware layer. It receives data from the transport layer. The data received from the transport layer is further analyzed and processed to eliminate unnecessary data and to retrieve meaningful and useful information. It provides and manages distinct types of services to the lower layers. It solves the issues related to managing large amounts of data, such as big data, and also helps in employing cloud computing (Zhong et al., 2015). Exhaustion and malware are the two common attacks that affect the working of this layer and thus affect the IoT performance. Exhaustion is used by the attacker to affect the smooth working of IoT. For example, the DoS attack is such a kind of attack in which the attacker sends several requests to the victim to block the network, so that the user cannot be able to access the network. Malware is a kind of attack that affects the privacy of users' data. Malware includes Trojans horses, spyware, worms, viruses, and much more (Wu et al., 2010).

3.2.3 Transport Layer

This layer is responsible for transferring the sensors' data from the perception layer to the processing layer, and vice versa. For this work, it uses different networks such as radio-frequency identification (RFID), local area network (LAN), wireless, Bluetooth, and near-field communication (NFC) (Zhong et al., 2015; Wu et al., 2010).

4 IoT Elements

IoT is divided into different stages said to be IoT elements that are required to deliver functions of IoT. The names are identification, sensing, communications, computations, services, and semantics.

4.1 Identification

Its role is in creating an identity for each and every object in the network. It also matches the services and the demands of the customers. Electronic product codes (EPC) and ubiquitous codes (ucode) are examples of identification methods (Vashi et al., 2017; Singh et al., 2020a).

4.2 Sensing

The sensing devices collect data from the objects of the network and send it to the data cloud, database, or data warehouse which is analyzed, and the course of action required for specific services is decided and executed (Vashi et al., 2017; Tripathi et al., 2020).

4.3 Communication

The heterogeneous nature of objects requires very smart technologies and services for communication. There are various communication protocols that are available in IoT to establish a seamless communication among heterogeneous objects together (Chae, 2019; Dubey et al., 2020). Some examples of communication protocols applicable for IoT are Bluetooth, Z-wave, Wi-Fi, IEEE 802.15, and other emerging standards.

4.4 Computation

The hardware and software both are part of the computational element (Sehgal et al., 2020). It includes hardware like microcontrollers, microprocessors, system on a chip (SoC), field-programmable gate arrays (FPGAs), and several real-time operating systems (RTOS) (Vashi et al., 2017).

4.5 Services

IoT services can be categorized into four different types: identity-related services, information aggregation services, collaborative-aware services, and ubiquitous services (Chae, 2019; Tripathi et al., 2020).

4.6 Semantics

Its role is to ensure that the data extracted from the system is received by the appropriate resources. In IoT, semantics means extracting knowledge from a different machine to provide the services required (Chae, 2019; Dubey et al., 2020).

5 IoT Features

The basic IoT features can be summarized under following points.

5.1 Interconnectivity

Any smart device should be connected to the infrastructure and the information system (Zhou et al., 2018).

5.2 Things-Related Services

The technology in the physical world and information in the world needs enhancements so as to meet the requirements of things related to servicing (Triantafyllou et al., 2018).

5.3 Heterogeneity

The devices in IoT systems are heterogeneous in nature as they are in different networks and on different platforms (Zhou et al., 2018).

5.4 Flexibility

The count of devices, the location, and the state of a device may change dynamically. A device in a sleeping state may go to wake up state and connected the device to a disconnected state on the next moment (Triantafyllou et al., 2018; Singh et al., 2020b).

5.5 Scalability

The system should be scalable in terms of number of devices and the amount of data to be handled (Zhou et al., 2018; Dubey et al., 2020).

6 Internet of Things for Smart Automation

6.1 Home Automation System

The goal of home automation is to provide controlling of different home appliances and services on fingertips which covers lighting solutions, home security, home entertainment, and optimizing energy use using energy conservation, etc., and many more (Humphries et al., 1997). IoT-based home automation uses networking protocols and cloud computing for automating all the services and the devices providing those services. IoT automation is also smart in the sense that it provides automation with the ease of installation and ease of use that too without needing physical connections, hence providing mobility features as well. IoT-based automation systems have sensors and servers (Bilger, 2005). These servers are on the Internet which controls a number of sensors installed at different locations and manages them perform data processing for automation. The basic home automation system is shown in Fig. 3. The working of the devices that are part of a home automation system will be described next.

6.1.1 Hub or Main Controller

The most important part to connect one or more sensors in any home automation system is the main controller also known as a gateway. The home router is connected with the main controller by Ethernet cable. The controller sends and receives the signals from IoT sensors and shares the output to the cloud network, and anyone can communicate with the

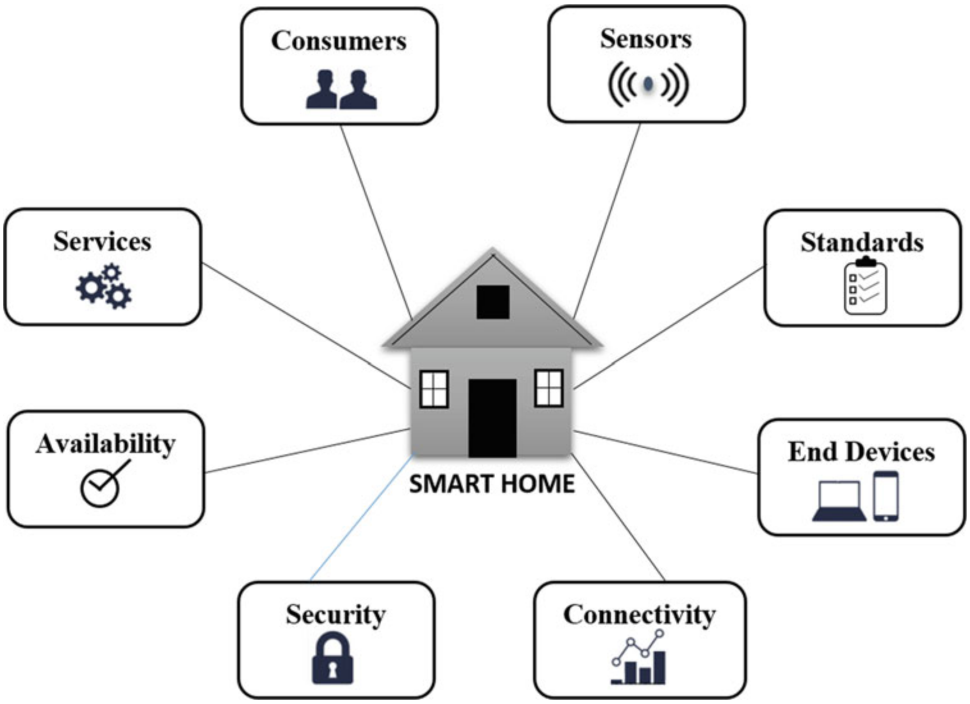


Fig. 3 Home automation system

controller from any remote location by using smartphones (Padikkapparambil et al., 2020). For this all to execute, you require a data package that connects your smartphone to cloud network and a reliable connection to the Internet. Many hubs produced by manufactures so far that are available there in the market for home automation are based on wireless communication protocols: Z-Wave, Zig-Bee, and Wi-Fi (Tripathi et al., 2020).

6.1.2 Devices

For automating the services in home-like lighting, entertainment, and security, the automation system needs many smart devices, i.e., sensing devices, and these devices need integration with the network and the controller via mesh topology. The main controller works as an exchange for communication between the devices in the network (Gupta, 2015). The controller helps the devices to cross-talk for example as soon as the doors and windows are closed after 7:00 PM, the lights inside the home need to be switched on. If the sensors and hubs are installed at very long distances, a special device named the signal repeater is installed in between which works as a sensor hub. In-home automation, smart plugs are commonly used as a sensor hub which helps the controller to transmit signals to devices that are at a long distance from the controller but in the vicinity of the sensor hub (Tanwar, 2020a).

6.1.3 Wireless Connections

Z-Wave, Zig-Bee, and Wi-Fi are the three wireless communication protocols that are used in almost all home automation systems today. The connections are always in a mesh topology, and the Z-Wave and Zig-Bee hubs are given a network ID which in turn is distributed on the rest of the sensors. Two sensors cannot communicate if they are having different network IDs (Huh et al., 2017). The signal is communicated through the shortest path available, i.e., if any device in the path is busy, a new shortest path is traced, and the signal is transmitted using this new path. The access of the data from anywhere, storage, and maintenance of it is done by cloud-based network systems which facilitates the users of the cloud network of sending the command to the controller from any location. Now to perform the required action, the signal is transmitted to the specific device, and when the action is performed, the cloud network is updated with the status of the action by the controller (Obaid et al., 2014; Unwala & Lu, 2017). IoT-based systems also have real-time monitoring feature as a result of which you can schedule the actions, events, and activities which are stored on the cloud network and are communicated to the controller or the hub as per their schedule. When the scheduled activity is performed, the device notified the controller about this and the controller updates the status of the activity on the cloud network helping the user to have an instant notification (Singh et al., 2020b). Every action cannot be triggered in a busy schedule, so IFTTT (IF This Then That) is there to help you out in this situation. IFTTT uses an automation system optimally for the smart lifestyle and energy saving by creating a cascading effect for example “IF” the temperature is above 30°; turn the ACs on, “IF” the time is 7:00 PM, switch the lights on and roll-down the curtains, etc.

6.2 Industrial Automation System

The industrial revolution paved the way for smart machinery and shifted the focus from skilled human resources which made the production process easy, quick, large in scale, and cost-effective (Braun, 2009). The repetitive tasks can be done by machines quickly, but the decision making and controlling still require highly skilled and experienced professionals. The basic model of the industrial automation system is depicted in Fig. 4.

The goal of the industrial automation system is to perform decision making and controlling crucial processes with the help of data processing and data analysis and reducing the human intervention which will make the processes cost-effective, decrease response time, and increase the throughput (Saha et al., 2017). A fully automated system uses smart sensors for the machine-to-machine communications and reduces the need for skilled manpower.

It is an estimate that the use of data analysis and artificial intelligence to automate the industries will increase productivity by 120% and decreasing the cost by 40%. The unpredictability of the operations is eliminated by using the data collected from intelligent sensing devices and making the whole system transparent in turnaround time and production (Tanwar, 2020a). In fully automated IoT systems, the controlling and monitoring is also automated; hence the need for active monitoring is also eliminated. The IoT-based automation is used in nearly all services and activities of the industry for example.

Tracking boiler temperature and sensing the movements in the machinery are the two major automation applications of retrofit sensors. The lego-block setup helps in machine-to-machine communications, and the complete workflow and processes can be automated by using a building block framework (Tanwar, 2020b). The IoT automation connects the system to the cloud and helps in monitoring the business parameters using smartphones or computer systems which also help in receiving real-time industry updates. Industry automation also provides services like real-time alerts and notifications about the workflow like the production is stopped or the output is very low, etc.

The use of GPS monitoring can provide the real-time tracking of the vehicles carrying goods and also sharing the status to the stakeholders. The production workflow can be monitored in real-time, and using the collected data, the productivity can be improved, and the processes can be optimized.

6.3 City Automation System

The population in the cities is growing on a large scale creating the challenges for services and activities like traffic control, pollution control, freshwater supply, sanitization monitoring, crime control, etc. (Saha et al., 2017). IoT solutions for cities have the potential of providing solutions to these problems and making the lifestyle of the residents better, safe, comfortable, and smarter (Lazaroiu & Roscia,

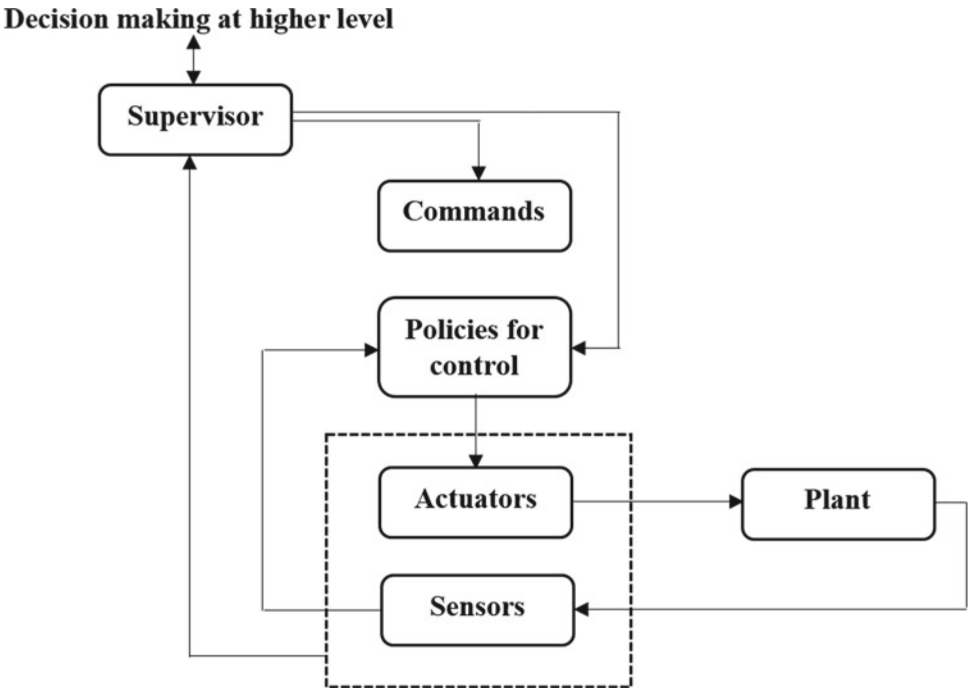


Fig. 4 Industrial automation system

2017). The areas in which IoT is used to make a city fully automated, i.e., smart city. Figure 5 shows a prototype of a city automation system.

6.3.1 Infrastructure

In future, most of the services will be provided by IoT-based systems, so the infrastructure of the cities should be developed wisely so as to meet the requirements of the IoT services and devices (Gope & Hwang, 2015). The future vehicles may be driverless and electric vehicles which will create specific needs in infrastructure, the lights may be intelligent enough to sense the vehicle's movement, i.e., if someone walks fast, it should manage its brightness and illuminations accordingly (Tanwar, 2020b).

6.3.2 Smart Lighting

Street lamps are connected with intelligent sensors, and those sensors are connected to a cloud management solution system (Sikder et al., 2018). The lighting solution collects data from illumination sensors, traffic system (people and vehicle movement), and integrating it with historical and contextual data that the smart lighting solution decides when to switch on, switch off, dim, or brighten the street lights. For example, if a vehicle or pedestrian passes, the traffic lights are automatically brighter (Al-Shammari et al., 2017).

6.3.3 Traffic Management

In cities, the automation system optimizes traffic by using sensors and GPS data from driver's smartphones; analysis of historical data provides an idea of future traffic congestions and efforts required to manage it (Al-Shammari et al., 2017). The location, speed of a vehicle, and the number of vehicles in that location can be monitored by using the data received from driver's smartphones and the red and green signals, and their timings are automatically decided by using that data (Vora et al., 2017). Examples are cities like Los Angeles that have intelligent traffic control systems in place and are developing a light management system that will react in real-time according to the traffic in the area.

6.3.4 Public Safety

The analytics, monitoring, and decision-making tools integrate data from social media, CCTV cameras, and the sensors around the city and predict the probable crime scenes that help the police to track the criminals and reduce the crime rates (Fraga-Lamas et al., 2016; Gupta et al., 2020).

6.3.5 Pollution Control

"The City Air Management Tool" a cloud-based tool developed by Siemens based on artificial neural networks collects the data in real time and with about 90% accuracy for costs the future emissions (Saha et al., 2017). It is based on MindSphere an operating system by Siemens for IoTs and may predict the future 3–5 days' emissions.

6.3.6 Smart Parking

Today, the concept of smart parking is a reality. It gets the idea of vehicles arriving and leaving and the area free for parking using GPS data and surface sensors on parking spots and tells the driver on his smartphone where he should move to get the closest parking space (Khanna & Anand, 2016).

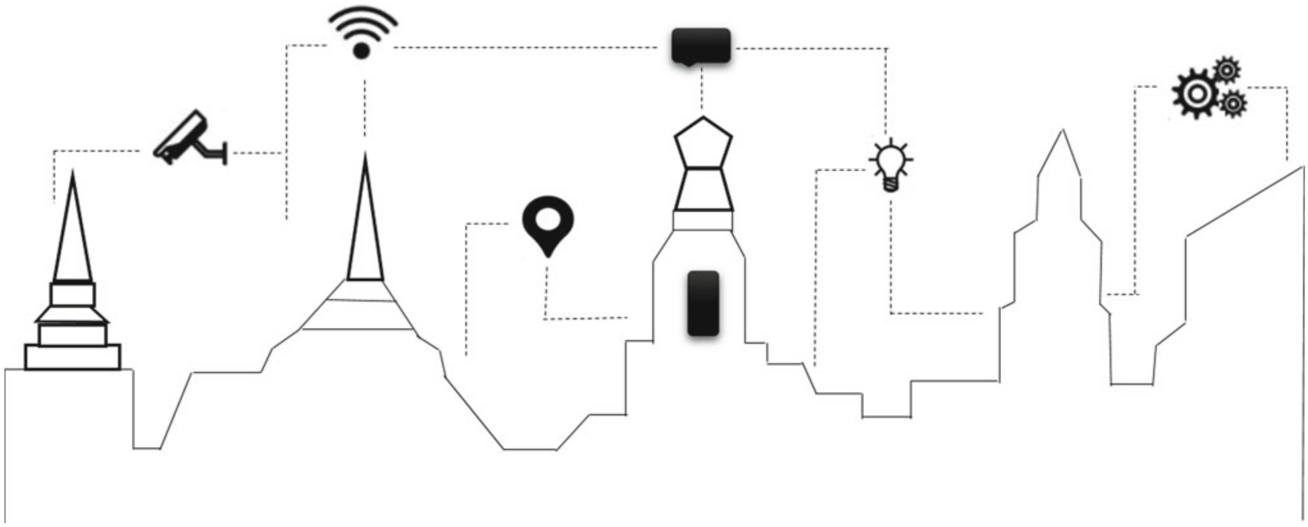


Fig. 5 City automation system

6.3.7 Sanitization Monitoring

To avoid wastes piling up, the waste containers have senses, and the monitoring system informs the truck drivers on their smartphones when a pre-decided threshold is reached (Prasad et al., 2015).

6.3.8 Public Transport

To achieve up to mark safety and punctuality, the data from smart sensors, ticket sales, and traffic automation systems can be used by smart public transport solutions. In London by using the data from motion sensors, ticket sales, and CCTV cameras, some train operators predict the trains loading up with the passengers (Sutar et al., 2016; Tripathi et al., 2020). The example is "A gun Shot Detection Solution" used in many cities in the U.S. that uses the data from microphone that are installed in the city and analyzing the data the cloud solution informs the police on their smart phones in real-time the location of the gunshot.

Thus, the use of IoT for smart cities is unlimited from education, restaurant, health care, manufacturing to fashion industries. The cloud-based nature of IoT solutions is efficient to provide a common smart city platform.

7 Internet of Things for Robots

The robots are going to play a vital role in a society in assisting people to accomplish the tasks in areas like health care, military, and industry, etc. The future of IoT integrated with robotics is going to be a tangible reality in our daily life. These technologies are going to assist us in every field of society. The Internet of Robots has a bright future as the IoT-aided robotics is going to create an eco-system where the IoT devices, human beings, and robots will cooperatively decide the protocols to share the data and services they want to provide or access (Ray, 2016). A number of issues are to be resolved and approaches to be finalized like architecture selection and design methodology selection, to make it happen. The capabilities of the robots of sensing, computing, and communicating can be enhanced many folds with the integration of robots and IoT and thus making the robots intelligent enough to solve the most critical problems. The intelligent sensors and objects, networking devices, and robots may create a worthy network infrastructure for the Internet of Robots.

7.1 Applications of IoT-Aided Robotics

7.1.1 Health Care

In health care, the IoT-aided robots are used to manage drug supplies and to monitor the patients and medical staff and equipment. A wireless body area network (WBAN) uses physiological sensors in collecting biological signals from a patient's body and sends it to a device that visualizes the data. In mobile-health systems, the doctors and the other medical staff can monitor the status of a patient who is at his home. The administration of drugs and monitoring of its effects will be a reality in the coming future (Bui & Zorzi, 2011). To help physical rehabilitation, a number of robotic systems have been developed, for example, BioMotionBot. Today, the robots are mainly used for rehabilitation and assistance to the patients, but with IoT-aided robotics, the applications of the robots in healthcare system will increase.

7.1.2 Industrial Plants

The research of today is to improve the use of robots in the industry by enhancing the services and actions performed by robots. This whole upgradation process will be very easy if the robots are supported by IoT technology and its intelligent devices. Robots equipped with artificial intelligence work more smartly and play a vital role in the industry as the human–robot interaction and coordination become much more effective (Breivold & Sandström, 2015). For industry applications, robot programming is the main concentration point as it has to cope with different innovations and frequency diversification of the product range. Every household is not having a robot today but for domestic services the robots such as cleaning robots across the globe. The research is going on to make the robots used today more intelligent so as to use them in public places like shopping malls, airports, railway stations, etc., for providing various services to customers and monitoring the complete surrounding.

In industries, the robots are very useful for critically dangerous areas like the area filled with fatal gas or liquid, the area inside a machine, or a furnace where i i's dangerous for a human being to work, etc. IoT-aided robots will be very effective and suitable for smart areas and industrial applications. The deployment of the smart objects across the industry campuses will help in capturing data, processing it, and get the task done by the robots by providing them the commands. In future, the IoT may enable the robots and smart objects across the globe to connect and communicate for providing a number of advanced services to customers changing the world and its life style manifolds.

7.1.3 Military Applications

The very first application of the robots in military applications was robot vehicles known as unmanned ground vehicles (UGVs) that are used for transportation. Today, the researchers are working on the concept of four-legged vehicles, BigDog capable of moving on rough surfaces (Wrona, 2015). It has also created the possibility of unmanned surface vehicles and unmanned underwater vehicles which will open the way of smooth transportation in naval areas. The basic requirement for this all to be effective is that the human and robot interaction and communication should be effective. The IoT-aided robots may provide various services and application for the military:

- Nuclear weapons can be deactivated automatically if they are in unsecure environment.
- Aircrafts and vehicles can be monitored without human intervention.
- Harmful chemicals and biological weapons can be detected automatically.
- Detection of intrusion in restricted areas.

7.2 Internet of Robotic Things Technologies

IoRTs are the things autonomous, intelligent, and complex things that are equipped with the technologies of robotics and artificial intelligence and use the platform of cloud computing. IoT architectures and autonomous architectures are integrated on the basis of some characteristics that are:

The first and main characteristic of interaction between "things" and devices, devices, and people are "Sensing." The IoT technologies along with IoRT need excellent sensing capabilities for the best interaction and performance of the automation system (Ray, 2016).

The next characteristic that is vital for IoRT and hence IoT services is "Actuating." It needs secure and reliable deployment of services to perform well in the IoT infrastructure floated around the globe (Simoens et al., 2018).

The loops or sequence of loops also known as "Control Loops" define the services and functions where control means the sequence of organized operations. Between sensing services and control mechanisms, well-defined interfaces should be installed, and security features should be visible in the interface architecture deployed (Ray, 2016).

The other capability that coordinates to offer services of the best quality throughout the IoT application life cycle is "Planning." The logic aligns the services and the resources, and on the basis of this logic, the planning is dependent on the workflow engine.

Robot–human interaction is established by robots using knowledge modeling and sensor information combination through "Perception." Perception makes robots more aware of the environment around it.

Using Cognition, robots become more intelligent with enhanced sensing and monitoring capabilities. Also, they receive the data, needed by the devices to execute the tasks. The device collects the data from the devices that it monitors and analyzes it to show the intelligence locally and in a distributed fashion (Simoens et al., 2018).

To provide facilities and services to the IoRT platform, the two most important components of the IoRT system are sensors and actuators. A robotic system that is a functional implementation of sensors and actuator services provides human–robot interaction service and uses external building blocks. Some robot hardware is microphones, radar, camera, etc. The properties of complex sensing and actuating is also inherited in IoRT from traditional robotics. Sophisticated sensors (ranging sensors and inertial sensors), as well as simple sensors (camera and microphone), both the sensors, are used by the methods provided by robotic science and technology.

7.3 The Future of Robots with IoT

The IoT devices need to do specific tasks while robots are required to perform the tasks in familiar and unprecedented situations too. When IoT, robotics, and machine learning integrated together, they can deal with such situations. To describe a smart robot, we can say that it performs almost all the tasks the humans can perform (Batth et al., 2018). Pneumatic robot arms that are controlled by remotes can be used to retrieve something after selecting it from a group of things or the hands of a person without any damage to him or anyone present there. The robots perform tasks efficiently and use the data inputs to learn to enhance their performance in performing similar tasks in the future. Such environments enable the robots not only in doing some work as per the given commands but also to help them in evolving with experience and perform some tasks in unexpected circumstances (Grieco et al., 2014).

Like a human being, if robots commit some mistake, they try leaning the ideas that ensure that they do not commit the same mistake in the future, and all this happens because of machine learning technology evolving today (Batth et al., 2018). Alongside their human counterparts, the more collaborative robots are working and helping the human counterpart in performing the tasks that are done in repetitions. For example, the robot transports goods from one place to another alongside human workers, i.e., the robots do not replace them but assist them.

To delve deeper into data, artificial intelligence and machine learning is used collaboratively. It will enable the machines and hence robots to take decisions and do predictions on the basis of the outcomes received after analyzing the data collected through different sources (Grieco et al., 2014). To improve performance, the IoT devices can be synchronized to enable them to talk to each other to create a smarter and much more aware environment. IoT devices and robots are having some similarities, as both need sensors to collect data and fast processing of that data to decide the response.

Table 1 IoT devices and robots

S. No.	Features/vectors	IoT	Robot
1	Sensing	Stationary sensing devices provide binary outputs	Multiple sensing devices provide complex outputs
2	Processing	Well-known method and algorithms process simple data signals	Neural networks are used to process complex data streams
3	Mobility	Stationary sensors	Robots are equipped with sensors, and the robot is mobile
4	Response	Need to act in response of well-defined situations	Require multiple choices of actions in response of a situation
5	Learning	Cannot learn and evolve	Learn and evolve to handle the new situations using machine learning
6	Design	The processing is done on clouds, and sensors are stationary, so it needs channel for communication between clouds and sensors	No need of communication network as such. The size and weight are the design attributes to concentrate upon

7.4 Industry 4.0 with IoT and Robots

If we talk about industry 4.0, the point of concentration is the manufacturing industry, and the cyber world along with the IoT technologies has changed the manufacturing industry-to-industry 4.0 (Strange & Zucchella, 2017). From enhancing operational efficiencies to customer services, IoT and cyber technology play a vital role. The IoT technology collects the data analyzed it and based on the outcomes of the analysis decides the future courses of action (Javaid & Haleem, 2019).

A Swedish-Swiss company ABB which produces industrial robots and provides a number of services to other companies is in many companies working in the field of energy and automation. The robots produced are not for common person's use but for manufacturing industries only (Javaid & Haleem, 2019). As the focus of all industries is on optimizing efficiency and services in terms of quantity and quality, the IoT plays a key role in avoiding the interruptions. The real-time servicing is performed with the help of the data collected by IoT. The business benefits are like:

1. The 24*7 service and that too without sending the services engineer at the point of site to detect the issue.
2. Optimizing the efficiency and minimizing the down time.
3. ABB launched a new service called "Connected Services" to launch new services.

Table 1 shows the comparison of IoT and robot on different features.

To extract the best out of the technologies, the best way is to use them in tandem, and if used with IoT, the world of robotics is going to experience a revolution in coming days.

8 Conclusion and Future Challenges

To conclude, we can say that the technologies when used in tandem can give the best outcomes. As up to 30% energy and efficiency can be saved by using smart devices, so ordinary devices are being replaced by smart devices needing the creation of a smart environment and space and hence a platform for IoT technology. Cybersecurity will pose a major challenge to IoT technology as with the passage of time number of IoT devices will grow to trillions. IEEE consumer electronics magazine recently pointed out that devices like home security cameras and thermostats are prone to hacking as they are very poorly protected. Availability, reliability, scalability, interoperability, mobility, performance, and management are other issues that will pose a big challenge to IoT.

References

Al-Shammari, B. K., Al-Aboody, N., & Al-Raweshidy, H. S. (2017). IoT traffic management and integration in the QoS supported network. *IEEE Internet of Things Journal, 5*(1), 352–370.

Batth, R. S., Nayyar, A., & Nagpal, A. (2018, August). Internet of robotic things: Driving intelligent robotics of future-concept, architecture, applications and technologies. In *2018 4th International Conference on Computing Sciences (ICCS)* (pp. 151–160). IEEE.

Bilger, B. (2005). Home automation system and method. U.S. Patent 6,912,429, Destiny Networks Inc.

Braun, S. D. (2009). Security system and method for an industrial automation system. U.S. Patent 7,530,113, Rockwell Automation Technologies Inc.

Breivold, H. P., & Sandström, K. (2015, December). Internet of things for industrial automation–challenges and technical solutions. In

2015 IEEE International Conference on Data Science and Data Intensive Systems (pp. 532–539). IEEE.

Bui, N., & Zorzi, M. (2011). October. Health care applications: A solution based on the internet of things. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies* (pp. 1–5).

Chae, B. K. (2019). The evolution of the internet of things (IoT): A computational text analysis. *Telecommunications Policy, 43*(10), 101848.

Dubey, S., Singh, P., Yadav, P., & Singh, K. K. (2020). Household waste management system using IoT and machine learning. *Procedia Computer Science, 167,* 1950–1959.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors, 16*(10), 1644.

Gartner, & McKinsey. https://www.machinedesign.com/automation-iiot/article/21836054/how-the-growing-impact-of-iot-is-automating-the-world.

Gope, P., & Hwang, T. (2015). Untraceable sensor movement in distributed IoT infrastructure. *IEEE Sensors Journal, 15*(9), 5340–5348.

Grieco, L. A., Rizzo, A., Colucci, S., Sicari, S., Piro, G., Di Paola, D., et al. (2014). IoT-aided robotics applications: Technological implications, target domains and open issues. *Computer Communications, 54,* 32–47.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Gupta, B. (2015). Discovering cloud-based services for IoT devices in an IoT network associated with a user. U.S. Patent Application 14/550,595, Qualcomm Inc.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE Access, 8,* 24746–24772.

Holtorf, C., & Piccini, A. (2009). *Contemporary archaeologies: Excavating now*.

Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In *2017 19th International Conference on Advanced Communication Technology (ICACT)* (pp. 464–467). IEEE.

Humphries, L. S., Rasmussen, G., Voita, D. L., & Pritchett, J. D. (1997). Home automation system. U.S. Patent 5,621,662, Intellinet Inc.

Javaid, M., & Haleem, A. (2019). Industry 4.0 applications in medical field: A brief review. *Current Medicine Research and Practice 9*(3), 102–109.

Jose, A. C., & Malekian, R. (2015). Smart home automation security: A literature review. *SmartCR, 5*(4), 269–285.

Khanna, A., & Anand, R. (2016, January). IoT based smart parking system. In *2016 International Conference on Internet of Things and Applications (IOTA)* (pp. 266–270). IEEE.

Lazaroiu, C., & Roscia, M. (2017, November). Smart district through IoT and blockchain. In *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)* (pp. 454–461). IEEE.

Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on internet and underlying issues. *Ad Hoc Networks, 28,* 68–90.

Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). *Advances in Computers, 117*(1), 129–164.

Obaid, T., Rashed, H., Abou-Elnour, A., Rehan, M., Saleh, M. M., & Tarique, M. (2014). ZigBee technology and its application in wireless home automation systems: A survey. *International Journal of Computer Networks & Communications, 6*(4), 115.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of things technologies for elderly health-care applications. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 217–243). Academic Press.

Prasad, A. N., Mamun, K. A., Islam, F. R., & Haqva, H. (2015, December). Smart water quality monitoring system. In *2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)* (pp. 1–6). IEEE.

Ray, P. P. (2016). Internet of robotic things: Concept, technologies, and challenges. *IEEE Access, 4,* 9489–9500.

Ren, J., Guo, H., Xu, C., & Zhang, Y. (2017). Serving at the edge: A scalable IoT architecture based on transparent computing. *IEEE Network, 31*(5), 96–105.

Robotics & The Cloud. http://www.systemantics.com/robotics-the-cloud/.

Saha, H. N., Auddy, S., Chatterjee, A., Pal, S., Pandey, S., Singh, R., Singh, R., Sharan, P., Banerjee, S., Ghosh, D., & Maity, A. (2017, August). Pollution control using internet of things (IoT). In *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)* (pp. 65–68). IEEE.

Saha, H. N., Auddy, S., Chatterjee, A., Pal, S., Sarkar, S., Singh, R., Singh, A. K., Sharan, P., Banerjee, S., Sarkar, R., & Maity, A. (2017, August). IoT solutions for smart cities. In *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)* (pp. 74–80). IEEE.

Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks, 5*(1), 1–17.

Sauter, T. (2010). The three generations of field-level networks—Evolution and compatibility issues. *IEEE Transactions on Industrial Electronics, 57*(11), 3585–3595.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Sikder, A. K., Acar, A., Aksu, H., Uluagac, A. S., Akkaya, K., & Conti, M. (2018, January). IoT-enabled smart lighting systems for smart cities. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 639–645). IEEE.

Simoens, P., Dragone, M., & Saffiotti, A. (2018). The internet of robotic things: A review of concept, added value and applications. *International Journal of Advanced Robotic Systems, 15*(1), 1729881418759424.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of things: From hype to reality. In *An industrial IoT approach for pharmaceutical industry growth* (Vol. 2, p. 191).

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020b). Internet of Things in pharma industry: Possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Academic Press.

Smartwatch. https://en.wikipedia.org/wiki/Smartwatch.

Strange, R., & Zucchella, A. (2017). Industry 4.0, global value chains and international business. *Multinational Business Review*.

Sutar, S. H., Koul, R., & Suryavanshi, R. (2016, January). Integration of smart phone and IOT for development of smart public transportation system. In *2016 International Conference on Internet of Things and Applications (IOTA)* (pp. 73–78). IEEE.

Tanwar, S. (2020a). *Fog computing for healthcare 4.0 environments: Technical, societal, and future implications, signals and communication technology*. Springer International Publishing, (pp. 1–622).

Tanwar, S. (2020b). *Fog data analytics for IoT applications—Next generation process model with state-of-the-art technologies, studies in big data* (Vol. 76, pp. 1–497). Springer International Publishing.

The Wall Street Journal. https://www.wsj.com/articles/google-to-buy-nest-labs-for-32-billion-1389648107.

Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. *Wireless Communications and Mobile Computing*.

Tripathi, A., Singh, A. K., Choudhary, P., Vashist, P. C., & Mishra, K. K. (2020). Significance of wireless technology in internet of things (IoT). In *Machine learning and cognitive computing for mobile communications and wireless networks* (p. 131).

Unwala, I., & Lu, J. (2017). IoT protocols: Z-wave and thread. *International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRSCE) 3*(11), 355–359.

Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017, February). Internet of things (IoT): A vision, architectural elements, and security issues. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (pp. 492–496). IEEE.

Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of things: Converging technologies for smart environments and integrated ecosystems*. River publishers.

Vora, J., Tanwar, S., Tyagi, S., Kumar, N., & Rodrigues, J. J. P. C. (2017). Home-based exercise system for patients using IoT enabled smart speaker. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian*, pp. 1–6.

Wrona, K. (2015, December). Securing the internet of things, a military perspective. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 502–507). IEEE.

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)* (Vol. 5, pp. V5–484). IEEE.

Zhong, C. L., Zhu, Z., & Huang, R. G. (2015, August). Study on the IOT architecture and gateway technology. In *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)* (pp. 196–199). IEEE.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal, 6*(2), 1606–1616.

Application of Internet of Thing and Cyber Physical System in Industry 4.0 Smart Manufacturing

Oluwakemi Christiana Abikoye, Amos Orenyi Bajeh,
Joseph Bamidele Awotunde, Ahmed Oloduowo Ameen,
Hammed Adeleye Mojeed, Muyideen Abdulraheem,
Idowu Dauda Oladipo, and Shakirat Aderonke Salihu

Abstract

The advent of Industry 4.0 has moved the manufacturing industry to recent models of Internet of Things (IoT), cyber physical systems (CPS), cloud manufacturing, fog computing, big data analytics, among others. Data has become more ubiquitous with the increase in the development of mobile and wireless networking technologies. Also, due to high expectations for productivity improvement, efficiency, and enabling innovative service through collaborative means, IoT is attracting much attention. CPS is the integration of computational objects in fitting together with the corporal biosphere and its procedures. CPSs are complicated manufacturing systems with the goal to combine and harmonize mechanism biosphere and industrial capability to the cyber computational space. Nevertheless, having thorough interconnectivity and a computational platform is essential for a practicable application of CPSs and smart factories. Smart manufacturing, also known as Industry 4.0 or Industry Internet of Things (IIoT), is increasingly becoming the common goal of various industrial and national strategies. For a better implementation of smart manufacturing, smart interconnection is one of the most significant issues. Current technologies, however, are not yet completely equipped for smart interconnection while working with heterogeneous hardware, fast setup, and delivery, as well as online service generation. In this chapter, the effects of IoT technology and CPS in the advancement and awareness of real-life smart manufacturing is addressed. An integrated IoT and CPS framework is recommended as a specification for researchers and industries toward the full realization of the potentials of IoT with CPS in the development of Industry 4.0 smart manufacturing technologies.

Keywords

Industry 4.0 • Internet of things • Cyber physical system • Smart factories • Cloud computing • Big data

1 Introduction

Industry is the section of an economy that manufactures material goods and equipment. Manufacturing industry has evolved over the years from mechanization to automation and smart processing that characterized the fourth industrial revolution, the Industry 4.0. This evolutionary leap has gone through several incremental revolutions with introduction of new and disruptive technologies from one revolution to another. The emergence of mechanical manufacturing machineries in the eighteenth century ushered in the first industrial revolution and was being used till nineteenth century (Drath & Horch, 2014). The second industrial revolution which began from the 1870s on is characterized by intensive use of electrical energy to achieve mass labor (Lasi et al., 2014). The "digital revolution" which emerged around 1970s

---

O. C. Abikoye · A. O. Bajeh (✉) · J. B. Awotunde · A. O. Ameen ·
H. A. Mojeed · M. Abdulraheem · I. D. Oladipo · S. A. Salihu
Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria
e-mail: bajehamos@unilorin.edu.ng

O. C. Abikoye
e-mail: abikoye.o@unilorin.edu.ng

J. B. Awotunde
e-mail: awotunde.jb@unilorin.edu.ng

A. O. Ameen
e-mail: ameen.ao@unilorin.edu.ng

H. A. Mojeed
e-mail: mojeed.ha@unilorin.edu.ng

M. Abdulraheem
e-mail: muyideen@unilorin.edu.ng

I. D. Oladipo
e-mail: odidowu@unilorin.edu.ng

S. A. Salihu
e-mail: salihu.sa@unilorin.edu.ng

K. K. Singh et al. (eds.), *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66222-6_14

is the third industrial revolution where advanced electronics and information technology were introduced in the manufacturing industry to achieve the automation of production processes (Lu, 2017). With all these technological advancements in the preceding revolutions, manufacturing industries has recently been faced with many requests for high adaptability and interoperability. To address this challenge, the developing German manufacturing industry in 2011 introduced into the manufacturing industry with the combination of Internet technologies and future-oriented technologies (i.e., smart objects) that depend on aggregation heterogeneous data and integration of domain knowledge (Lasi et al., 2014; Lu, 2017). This modern advancement resulted in a new fundamental paradigm shift in industrial production; the fourth industrial revolution called Industry 4.0.

The main goals of Industry 4.0 include the provision of smart manufacturing through the integration of embedded intelligent computational component in order to achieve higher level of automation and to enable decentralized production processes by establishing smart communication between people, machines, and resources toward the realization of a higher level of productivity and operational efficiency (Lu, 2017). The smart production of Industry 4.0 is realized with the use cyber physical system (CPS). CPSs are systems of collaborating computational entities connected with the physical world, providing and using simultaneously, data-accessing and data-processing services available on the Internet (Monostori et al., 2016). The functions of CPS within the Industry 4.0 are to enhance robust and dynamic production, and to provide modular and efficient manufacturing platform where products control their own manufacturing process (Hermann et al., 2016).

Moreover, the smart communication of the Industry 4.0 is achieved with the use of sophisticated networking technologies such as sensor networks, cloud computing, edge computing, and so on. However, due to the proliferation of tiny computational entities referred to as “smart objects” or “things,” Internet of Thing (IoT) has been identified as the key player in providing the smart communications between the components of Industry 4.0 (Zhang et al., 2018). The IoT primarily enables uniquely addressable “things” such as RFID, sensors, actuators, and mobile phones to interact with each other and neighboring ‘smart’ components to carry out computational processes intelligently.

Moreover, considering the new technological advancement in Industry 4.0, CPSs as the core components are expected to be equipped with multiple sensors and actuators capable of storing and analyzing data, and be interconnected via IoT sensor networks to provide interoperability, adaptability, operational efficiency, and knowledge integration of the smart manufacturing. Nevertheless, the adoption of this novel technological advancement in manufacturing companies is still a current challenge for industries, because their application will enforce a complete reconfiguration of the entire company. This Chapter closes this gap by analyzing proposed CPS-IoT integration/fusion models and provide specifications and recommendation for its adoption.

The remaining part of the chapter is organized as follows. Section 2 introduces Industry 4.0 and smart manufacturing. Section 3 discusses CPS with focus on its architecture, application domains, and supporting technologies. Section 4 presents IoT and its architecture. Application of CPS and IoT are discussed in Sect. 5. Different integrated CPS-IoT models proposed in the literature are analyzed in Sect. 6 while some open research issues are also discussed. Section 7 concludes the chapter.

2 Industry 4.0 and Smart Manufacturing

As revealed by Lu (2017), there is no commonly accepted definition for Industry 4.0 because there are diverse definitions given by different authors. Notable is the precise definition by Hermann et al. (2016); “a collective term for technologies and concepts of value chain organization.” A more elaborate definition is given by Consortium II (2019) in the internet Fact Sheet as “integrating advanced physical machines and facilities with networked sensors and applications for forecasting, monitoring, and preparing positive market and social outcomes.” Basically, Industry 4.0 introduced ICT computerization, automation, intelligent processing, and smart interconnection into the traditional manufacturing industry. It represents the fourth industrial revolution characterized by cyber physical systems’ (CPSs’) production and decentralized manufacturing processes over smart network connectivity.

The words “Industry 4.0 and Smart Industry” represent the industrial transition from standalone embedded systems to interconnected CPS (Kagermann & Wahlster, 2016). Lasi et al. (2014) described Industry 4.0’s basic features as including smart factory, self-organization, CPS, the intelligent procurement and distribution systems, smart goods and services production systems, changes to human needs, and collaborative social responsibility. Industry 4.0 is planned for distributed production by connected facilities in the on-demand manufacturing universal industrial network to achieve customization and resource efficiency (Brettel et al., 2014). This has major impacts on manufacturers and consumers alike. From the manufacturer’s point of view, it needs very little human involvement, because computers reconfigure facilities automatically to adapt to the changing production plan.

2.1 Design Principles of Industry 4.0

Hermann et al. (2016) identified four (4) design principles that the concept of Industry 4.0 is generally based on. These philosophies suggest a universal framework to the core necessities of building Industry 4.0 systems and applications. The principles are outlined in the following.

Interconnection and interoperability

In Industry 4.0, Internet of Everything (IOE) is formed by interconnecting machines, devices, equipment, sensors, and people over wireless communication networks and IoT. This allows for interoperability among the Industry 4.0 components and smart factories as well as plays a prominent role in the increasing interaction that enhances ubiquitous computing and Internet access. For flexible interconnection of components, common communication standards are of great importance, and this leads to modularity in Industry 4.0 design. Such standards give room for dynamic integration of modular machines from different factories. Several technologies for instance IoT, cloud computing, fog computing, and CPS are deployed to achieve this design principle.

Decentralization

Industry 4.0 systems and applications are built to make decentralized decision. The participants in the Industry 4.0 carry out their processes and tasks in autonomous manner within the context of interconnection/interoperability as well as transparent information sharing from internal and external production unit. Only in necessitating exception, tasks are transferred to the central or higher processing systems for completion. Decentralization in Industry 4.0 is realized with the help of CPS using embedded computers, sensors and actors, and edge/fog computing that utilizes local and global information at a node level. These technologies autonomously control and monitor the physical world.

Information Transparency

Information transparency is achieved when there is a merge among the actual world and the cybernetic biosphere which is achieved by the utilization of CPS and IoT in Industry 4.0. The merging specifies how context-aware information are shared transparently among participant in the smart manufacturing. Since the context-aware evidence is required for smart factory members to make choices smartly, schemes achieve their functions using information gathered from the virtual and real world. The merging of the real and virtual world is achieved by connecting sensor data with digitalized machine models, thereby building a cybernetic replica of the real biosphere that allows a novel method of information transparency.

Technical Assistance

In Industry 4.0, smart machines, equipment, and devices aggregate and analyze information to help humans make informed decisions. This assumed characteristic of smart factory applications and systems shifts the role of humans from operator of machines to strategic decision makers. CPS and IoT enable smart factories to provide technical assistance to humans through human–machine collaboration support.

All technologies that could enhance smart manufacturing for instance smart strategy, smart machining, smart controller, smart managing, smart connections, and smart setting up, are included as mechanisms of Industry 4.0 (Zheng et al., 2018). Lu (2017) presented a conceptual architecture of Industry 4.0 interoperability as depicted in Fig. 1.

At the core of the architecture is the cyber physical system (CPS) that handles smart processes and carries out actions smartly in the real-world environment. It also included the component applications of Industry 4.0 built on the CPSs. The mechanisms include smart city, smart product, smart, smart grid, smart transportation, smart facility, smart home and building, and smart factory and manufacturing. These components are connected via integrated communication links which include smart Internet of Things, integrated services, integrated people, and heterogeneous integrated data. The design structured the interoperability of Industry 4.0 into four levels of interoperability that are institutional (organizational), functional (applicable), technological, and semantic. This also outlined eight principles suitable for Industry 4.0 including accessibility, subsidiarity, protection, multilingualism, open source software, privacy, the use of open standards, and multilateral solutions.

2.2 Core Technological Pillars of Industry 4.0 Smart Manufacturing

The main goal of Industry 4.0 is to foster smart manufacturing by forming the heart of smart factory. It is the modern technological revolution in the industry that builds smart factories. Smart factory is an autonomous manufacturing industry where smart machines equipped with CPS communicate over the IoT operate to build smart products. To achieve smart manufacturing or factories, Kumar and Nayyar (2020) identified nine core technological pillars incorporated by the Industry 4.0. These technologies are briefly discussed as follows:

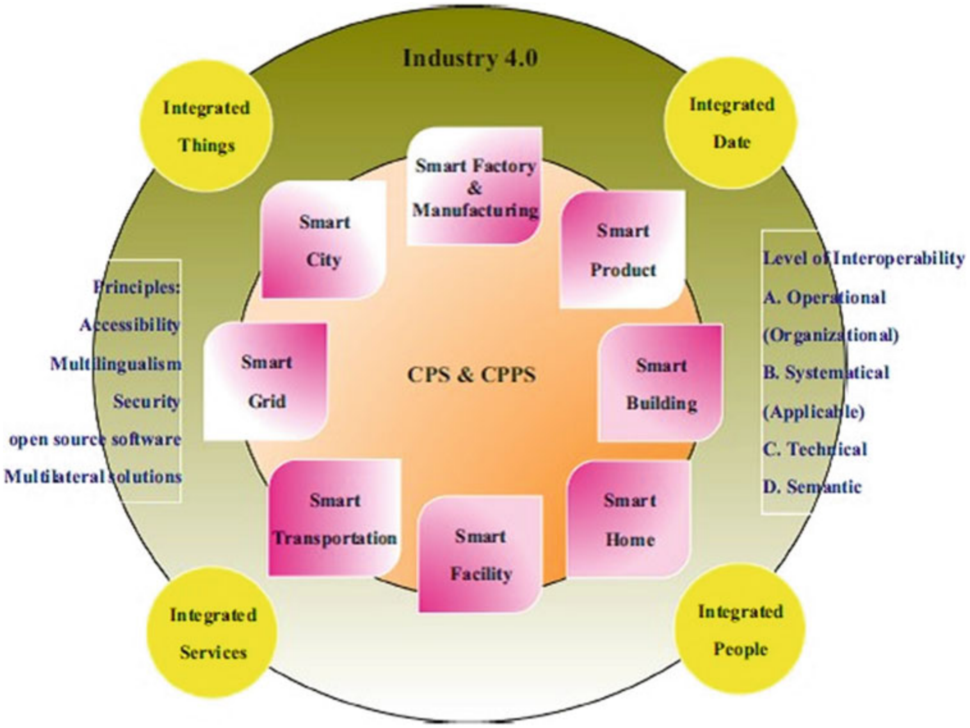


Fig. 1 An architectural framework for Industry 4.0 (Lu 2017)

Cyber Physical System (CPS)

CPS forms the core technology of Industry 4.0 which provides a connection between the manufacturing industries and the physical world with the use of embedded smart systems in production machineries. It merges with the IoT to connect the physical world with the virtual manufacturing world. More details on the design and architecture of CPS are discussed in Sect. 3.

Industrial Internet of Things (IIoT)

IoT basically is a ubiquitous network of sensors that gather data from the physical environment and communicate to aid intelligent and autonomous processes. It is primarily developed to simplify the machine-to-machine communications. The IoT in Industry 4.0 provides the sensing of the physical world for CPS by forming an interface for environmental data collection between the cyber manufacturing world and the physical world. IIOT is a subdivision of IoT with a special focus on industrial automation (Kumar & Nayyar, 2020). IoT in Industry 4.0 is discussed in details in Sect. 4.

Big Data Analytics

Big data analytics is applied in Industry 4.0 to analyze the vast amount of heterogeneous and unstructured data gathered by the CPS and IoT devices for speedy processing and smart decision making. The benefits of utilizing big data analytics by smart manufacturing companies include optimized production process, cost reduction, improved operational process, and increased profits (Kumar & Nayyar, 2020).

Advanced Robots

Robots, especially collaborative robotics (Cobot), form an essential part of the Industry 4.0 which is integrated to the smart factories for monitoring the conditions of machines and diagnosing machine failures. The emergence of Cobots, a networked group of robots that operate in a cooperative manner, has given rise to the concept of Internet of Robotics Things (IoRT). The IoRT within the Industry 4.0 provides machinery maintenance task and hard labor assistance.

Cloud Computing

Cloud computing is an enabling technology of the Industry 4.0 providing an online dynamic memory allocation and resource sharing for smart factories. Cloud computing provides hardware, software, and infrastructure resources for Industry 4.0 smart factories to enhance parallel processing and real-time data analysis. In particular, the big data analytics of the Industry 4.0 usually reside and rely on resources provided by the cloud computing technologies.

Horizontal and Vertical Integration

As evident in its various architectures (see Fig. 1), Industry 4.0 integrates things (devices, machinery, CPS, IoT sensors, actuators, robots, etc.), data (heterogeneous, structured, unstructured), people (producer, retailer, customer, operator, end user, etc.), and services (communications, networking, data analysis, real-time processes, ubiquitous computing, etc.). Industry 4.0 therefore possesses both horizontal and vertical system integration to make the manufacturing process smarter and more optimized.

Cyber Security

The horizontal and vertical integration of devices, people, services, and data in Industry 4.0 poses a security challenge as virtually everything is connected. Strong cyber security protocols are enforced in the Industry 4.0 to protect information and system from theft and protect hardware, software, and services from damage, unauthorized access, or disruption. Consequently, proper monitoring of the smart manufacturing processes is required to detect intrusion and prevent attack, a feature which is provided by the cyber security technology of the Industry 4.0.

Augmented Reality

Augmented reality provides virtualization of processes in Industry 4.0 smart manufacturing. Complex manufacturing procedures can be modeled with augmented reality before the actual production. The virtual models are more understandable and easily shareable within the production life circle.

3D Printing

3D printing represents the digitalization of products manufactured in the smart factory. It presents the manufactured product in a more customized way during production. With the help of augmented technologies, 3D printing will aid the production of customized and personalized product in the Industry 4.0 smart factories.

3 Cyber Physical System

Cyber physical computing has caught the attention of industry IT engineers in the twenty-first century (Hahanov, 2018). The cyber physical environment depends on big data centers, integrated knowledge, services, and applications which is keen on monitoring and managing processes and everything smart in digital real space with the goal of granting high standards of human life, and preserving natural resources and energy for generations to come. Recent improvements in cyber electronics have led to a notable increase in the number of applications that fuses the cyber systems with the real world, leading to what is known as cyber physical system (CPS).

According to Gunes et al. (2014), the cyber physical system (CPS) is defined as “a term describing a broad range of complex, multi-disciplinary, physically-aware next-generation engineered system that fuses embedded computing technologies (cyber part) into the physical world.” CPS refers to the physical manufacturing systems with embedded processors, actuators, and sensors that can be managed by a network of computers. This kind of system possesses feedback loops which have effects on computing procedures and improve adjustability, flexibility, extensibility, and safety of physical facilities (Lee, 2008). While CPS and Industry 4.0 are used synonymously in most instances, they are, in fact, two distinct words with a few similarities. At one hand, CPS recognized as a significant aspect of Industry 4.0, can also be extended to other fields such as education, military, and transportation. At the other hand, Industry 4.0 is not just the collaboration of physical and digital systems, but encompasses the complete business cycle from natural resource selection, part development, and product manufacturing to customer support and customer relationship management (Xu & Duan, 2019).

CPS focuses on linking the real world (physical world) to the cybernetic world, integrating and analyzing real-world and virtual-world knowledge (information) after interaction, and feedback on real-world data analysis. This connects the physical world to the cyber world with several ICTs, centered on cloud computing, fog/edge computing, and analytics of big data. This creates a very multifaceted and vast platforms which necessitates the fitting together of several corporal provinces and the dispensation of a huge volume of data.

In addition to sensor technologies, it is important to simultaneously develop and integrate different technologies, such as actuators, protection technologies, SW optimization, artificial intelligence, and data collection and analysis technologies. The cyber physical system interface consists of physical and cyber ports, through which it is incorporated with other components in order to interact effectively with these components to achieve the higher level of behavior needed at the sub-system or system level. Similar to CPS are other concepts such as Digital Twin (DT), CPPS (Tao et al., 2019).

The integration process of the components of physical systems is a major challenge as it directly affects the system’s quality properties such as maintainability, functionality, extensibility, adaptability, and versatility. Hehenberger et al. (2016) identified six components that make up CPS; corporeal world, transducers, control mechanisms, data analytics fundamentals, computation fundamentals, and communication mechanisms.

3.1 CPS Architecture

Sztipanovits et al. (2012) presented a three-layer architecture for CPS (see Fig. 2) consisting of the physical, platform, and software layers. The physical layer is composed of collection of smart objects that interact in the physical world. The platform layer involves the pervasive sensing elements that provide the physical layer with some sort of communication and data exchange capability to react to changes in the environment. The upper software layer comprises the applications, control algorithms, and methodologies that abstract the processes of the platform layer and interfaces the user directly.

A more elaborate and holistic architecture of CPS in a networked environment is presented in Bordel et al., (2017) as shown in Fig. 3. The architecture is composed of the physical world accessed via a network of sensor nodes as an architectural component. The network of sensor nodes transfers the collected data to the cyber system composing of CPS via communication networks which may sometimes include control and data analytics components. The CPS uses the gathered information to make informed decision and sends command via the communication links to the network of actuator nodes. The actuator node is the component that interacts with the physical world by carrying out the corresponding action embedded in the command received from the CPS. Similar to this, architecture is the one presented in Gunes et al. (2014). Based on this architectural framework, CPS systems need to be built taking into account the state-of-the-art technology, relevant system-level specifications, and complete effect on the actual world.

3.2 Application Domains of CPS

CPS has broad applications in production structures, medical operations and monitoring schemes, traffic control and protection, military systems, power generation and circulation, etc. (Lee, 2008). More specifically, Gunes et al. (2014) identified seven different domains and their respective applications where CPS has been widely employed. The domains and applications are:

(a) **Critical Infrastructure**: Critical infrastructure represents the distribution and management of basic national amenities such as water supply, electricity grid, oil exploration, and so on. CPS can be applied for the monitoring and maintenance of the machineries used in the various critical infrastructures. For example, in oil exploration, CPS can be adopted to monitor the oil level of the well and to carry out maintenance procedure to reduce oil spillage.

(b) **Health Care**: The modern health care systems are transiting to personalized heath management where patients are monitored and managed by machines even in the comfort of patient home. CPS is expected to be applied to monitor and manage patients' health condition by sensing the condition of the patients and provide feedbacks to physicians for proper medical advice and prescription.

(c) **Emergency Response**: Ensuring public safety and protecting nature and valuable infrastructures is an important function of any nation. In modern world, CPSs are expected to be applied to ensure safety of the

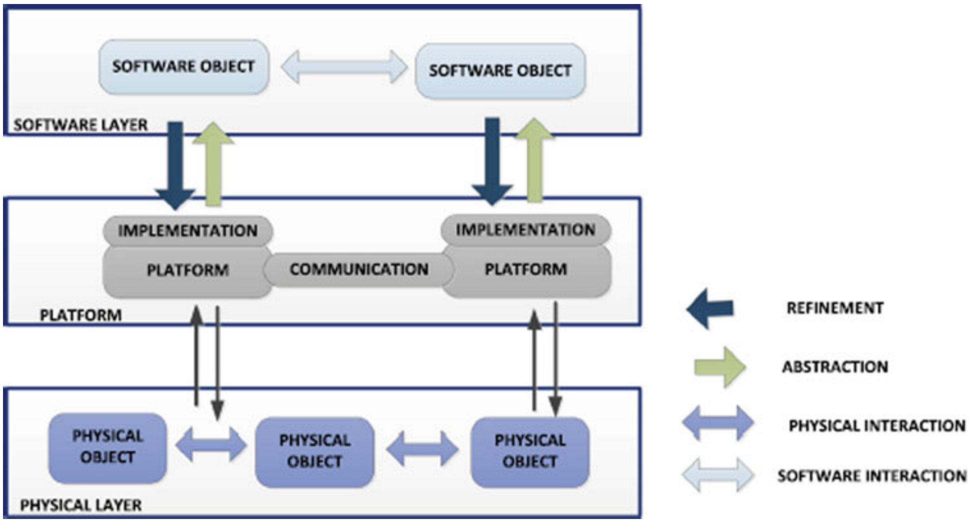


Fig. 2 A three-layer CPS architecture (Sztipanovits et al. 2012)

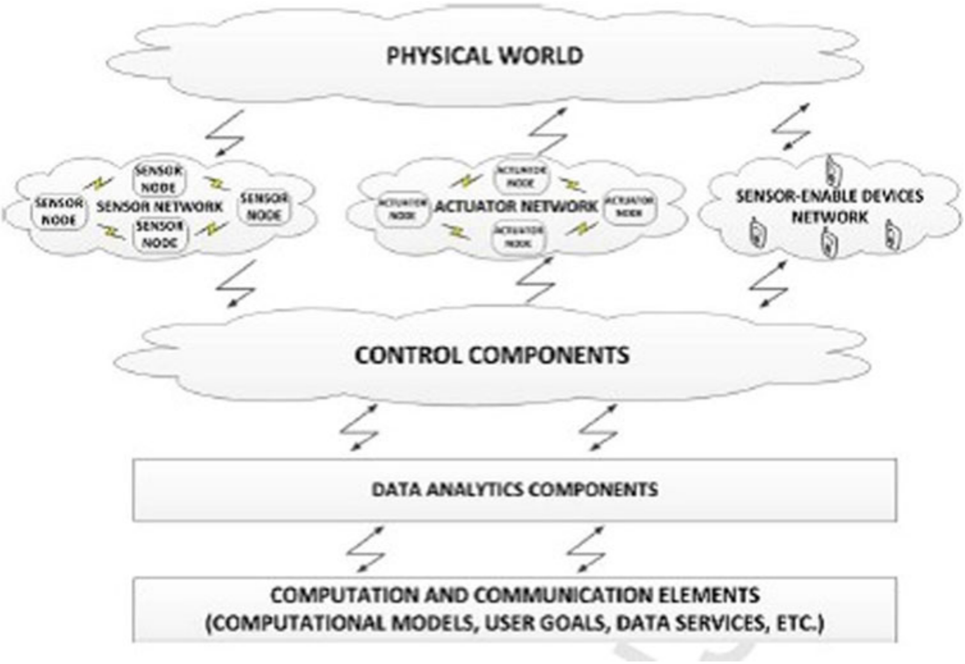


Fig. 3 A holistic view of CPS architecture (Bordel et al. 2017)

people as they are embedded in the physical world to monitor all kind of autonomous system and make smart decision during emergency situation to reduce the effect of disasters be it natural or man-made.

(d) **Intelligent Transportation**: The emergence of autonomous and self-driving vehicles calls for intelligent traffic management to ensure safety. Real-time vehicle traffic management, vehicle scheduling, and coordination can be handled by CPS through their sensing capability and smart processing. For example, the traffic control system equipped with a CPS could detect the existence of traffic and free space for passenger to plan their root and even communicate same with the vehicles.

(e) **Air Transportation**: Aircraft operation management systems and traffic control system are another area where CPS is expected to provide enhancement and optimization. CPS can gather traffic and weather information from the physical environment which can be sent to the aircraft for the pilot to make informed decision. This can reduce to the barest minimum the probability of crashing and landing problem often experience in air transportation.

(f) **Robotic Service**: CPS in particular provides assistive support for robots in the smart environments. CPS can process intelligently; data are received from sensors, and send commands to robots which serves as actuators to carry out some action and responds to changes in the environment. CPS can cooperate with the robots to ensure the welfare of the people and provide supportive services.

(g) **Smart Manufacturing**: CPS has found more application in the manufacturing industry. They are embedded into the machineries to sense the environment, controls the production process and carry out optimization of goods production and services delivery. CPS turns conventional factories to smart factories.

3.3 Supporting Technologies for CPS

Cloud Computing

Cloud computing is a computing platform that supports—in its diverse models—outsourcing of user's information computing services (Ruhse & Baturova, 2012). It is primarily a virtual combination of hardware and software environment provided via the Internet with a usage-bound subscription for the delivering of scalable computing services to concurrent users. Notably, the important basic attribute of cloud computing is the shared usage of computing resources by more than one customer. Moreover, cloud computing is considered as a paradigm change in information computing as its deployment requires important strategic decisions (Böhm et al., 2011). Cloud systems enables the transition from conventional standalone software products to service-oriented online software solutions. While there are different types of cloud computing models, the US National Institute of Standards and Technology (Mell & Grance, 2011) categorized cloud computing service models into Infrastructure as a Service (IaaS), Platform as a Service

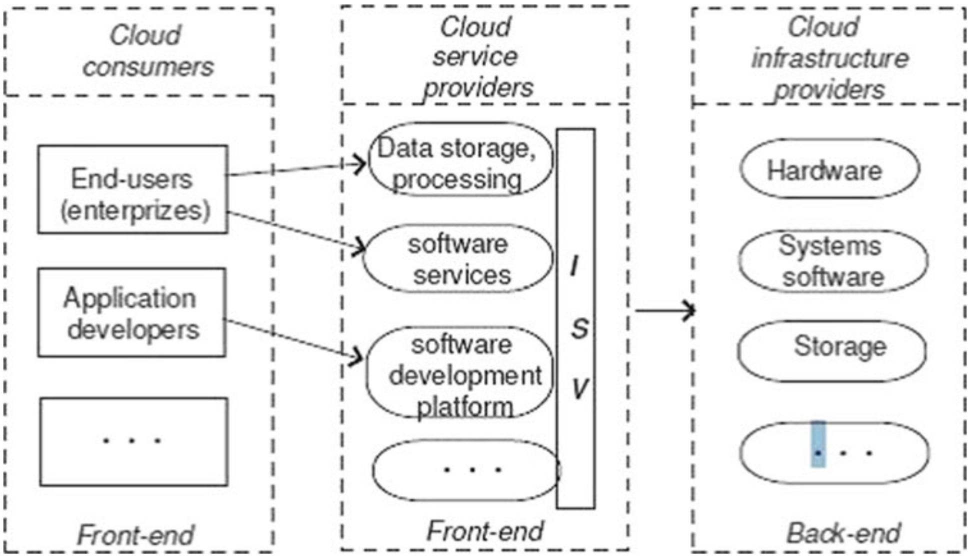


Fig. 4 Levels of abstraction of cloud computing (Hyseni et al., 2016)

(PaaS), and Software as a Service (SaaS). It also categorized cloud computing deployment models as: private, community, public, and hybrid. Figure 4 shows the levels of abstraction in cloud computing.

Consequently, cloud computing users benefit from the ever-available virtually unlimited computing resources, removal of upfront commitment, and the ability to pay on demand in short-term basis for the use of the resources. Numerous organizations are becoming more interested in cloud computing due to low-cost services that it offers and smart manufacturing of Industry 4.0 is not left out.

In Industry 4.0, cloud computing provides powerful platform service for integrating industrial IoT networks (Lu, 2017). Shih et al. (2016) opined the use of cloud services as the main host of collected data and intelligent decision in CPS/IoT smart cities in order to reduce the overhead of managing the services. Tu et al. (2016) also suggested that the use of cloud computing in distributed processing makes the manufacturing system more reliable as it can avoid a single point of failure and ensures scalability with increased production processes and product types for hybrid production lines.

Fog/edge Computing

Fog computing node acts as a small virtual data center within a very large network to provide the processor, configured hardware resources, and network services for applications running in a shared or ubiquitous environment (Singh et al., 2020b). Fog or edge computing has been shown to support the development of CPS by providing fast decentralized processing facilities and applications. O'donovan et al. (2018) proposed an industrialized cyber physical architecture built on the new fog computing framework that could integrate manufacturing-ready mechanism knowledge representations into manufacturing procedures to conform to Industry 4.0 design issues related to decentralization, efficiency, safety, and dependability. The cloud framework holds manufacturing-ready machine learning models programmed as predictive modeling markup language (PMML) for various manufacturing applications (e.g., machinery prognostics), which are circulated and performed by fog nodes installed inside the local network of the facility. Comparison was made between the stability and accuracy of the applied cyber physical fog interface and that of a standard cloud system. The results revealed that the fog interface recorded slightly lesser extreme implementation periods than the cloud interface, with variations in maximum latency estimated at 92.9%, 99.4%, 67.7%, and 91.0% for 50 connections, 100 connections, 250 connections, and 500 connections, respectively. These variations can be due to regional and entrenched fog processing features, which have less network routing and remote communication dependencies.

Big Data analytics

Big data is a paragliding term used to describe any method that handles vast volumes of data, including data collection, transmission, storage, discovery, analysis, simulation, protection, and privacy. The scale of big data is a continually evolving concept growing from Terabytes in 2005 to Zettabye in 2017, which is generally characterized by the volume of data to be stored within a tolerable period of time in a widely used device. Data collection and delivery in the big data world is important for the development of self-conscious and self-learning machines. Big data as a utility method is considered to control data capacity and speed all through the data gathering process and is proficient of collecting and briefing computer activity awareness under various operating conditions in order to generate evidence that grows for a certain period (Marini & Bianchini, 2016).

Since CPS produces an enormous stream of data, big data analytics are needed to conduct detailed data analysis and obtain valuable insights to help optimize device scalability, stability, and productivity (Xu & Duan, 2019). Nonetheless, the incorporation of the vast capacity and extensive diversity of data produced from manifold sources into the CPS is difficult, due to the fact that big data in CPS is not appropriate for traditional electronic processing results (Zhang, 2014). There are usually two major technical components, network infrastructures and data processing, to manage CPS big data challenge in Industry 4.0, as shown in Fig. 5. Network infrastructures track communications in order to ensure real-time contact between physical components and computer apps, while data analytics in Industry 4.0 focuses on increasing product customization and resource performance. However, some significant CPS issues including scalability, reliability, and durability are related to both data analytics and network infrastructures.

Many studies have examined the application of big data in cyber physical structures; a CPS that utilizes vast volumes of multifaceted data to accomplish their purposes. Zhang (2014) developed a method to incorporating the architecture analysis and design language (AADL), ModelicaML, as well as hybrid relation calculus for the development of big data-driven CPS. Zhang (2014) as well suggested AADL-based big data-driven CPS for applying device specifications. Also, Zhang et al. (2015) suggested—as an Urban CPS—a series of urban infrastructures for instance telecommunications, public transportation, and truck networks and develop as well as deploy urban CPS to effectively incorporate diverse models built on multi-origin structure data. Because of the absence of current logic technology and software applications related to publications for quest, decision making, and pattern recognition in the big data field, Hahanov et al. (2015) proposed a qubit-vector computing automation model focused on eliminating arithmetic solutions that optimizes performance and hardware complexity.

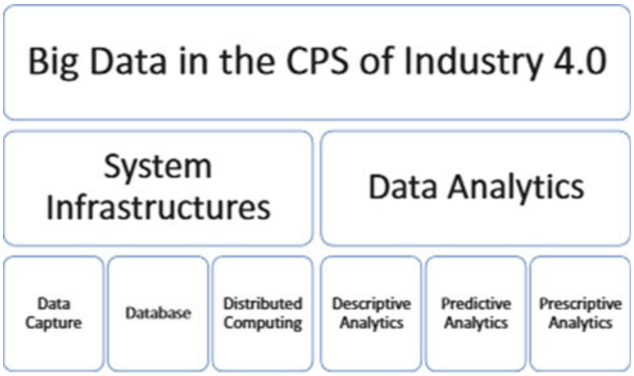


Fig. 5 Big data and CPS (Xu & Duan, 2019)

4 Internet of Things (IoT)

As described by Borgia (2014), "IoT refers to a new concept consisting of a continuum of specific addressable objects that interact with each other to form a complex network across the world." It is a model for interconnected devices with tracking, sensing, processing, and analyzing capabilities. It also provides a paradigm through which digital and physical objects can be interlinked and intercommunicate to provide some domain-specific services. IoT specifically transforms real-world objects into smart objects which can sense their environments with the use of RFID (and other sensing technologies) and communicate them accordingly.

Many IoT devices combined embedded systems, mobile computing, cloud computing, low-price hardware, big data, and other technological advancements in order to provide data storage, network connectivity, and computing functionality for equipment that hitherto lacked them. The ability of IoT to provide network connectivity for equipment has brought about new technological advancements such as remote equipment configuration, monitoring, and troubleshooting. IoT is also equipped with the powerful technologies to analyze heterogeneous data collected from the environment to make informed decisions, interact intelligently with the physical world, and predict future occurrence of events.

Presented by Borgia (2014) is a three-phase architecture (see Fig. 6) in which the physical-cyber universe communication takes place with the IoT. The three phases are described in the following.

1. **Collection phase**: comprises the technologies that senses the physical world and the technologies for the collection of real-time physical data from the environment. Technologies such as RFID, sensors, actuators, smart camera, smart phones, GPS terminals, and so on are used to identify objects in the physical world and perform the sensing of physical parameters such as temperature, pressure, motion, lux, and so on, while short-range communication technologies including ZigBee, Bluetooth, IEEE 802.15.4, NFC and so on are employed for data collection.
2. **Transmission phase**: comprises the long-range communication networks and communication protocols that help in transferring the collected data from phase 1 to different external servers and applications. The long-range communication networks are accessed through gateways and heterogeneous technologies such

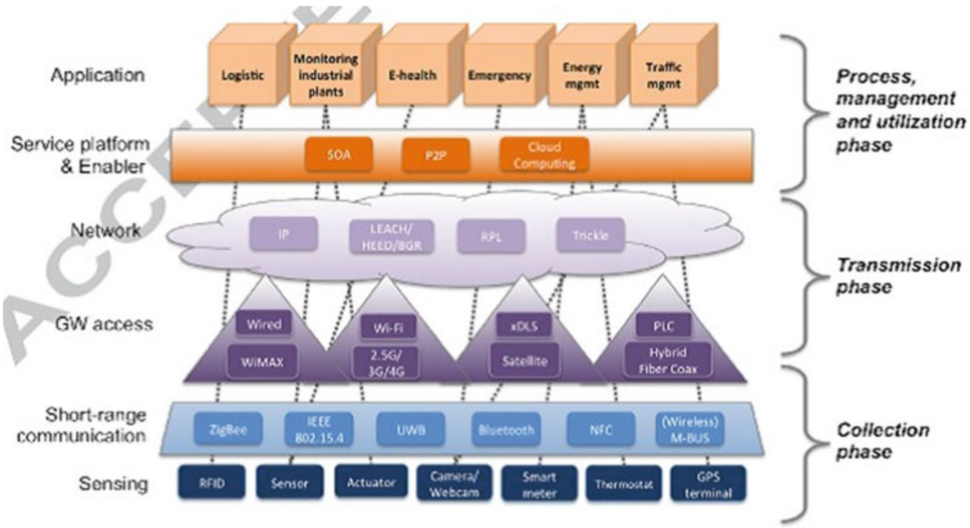


Fig. 6 IoT phases and applications (Borgia, 2014)

as wired WiMAX, Wi-Fi (2.5G/3G/4G), satellite networks, and PLC hybrid fiber coax. Communication protocols such as IP, LEACH, RPL, and Trickle are used for addressing and routing.

3. **Process management and utilization phase**: deals with the analysis of information flows, data forwarding, and feedbacks control for applications and services. This phase comprises the service platform layer such as cloud computing, SOA, and P2P which are responsible for aggregating data and perform semantic analysis, and the user applications such as logistics, e-health, traffic management, and industrial processes monitoring are responsible for data utilization.

Various application areas of IoT have been identified (Sehgal et al., 2020; Padikkapparambil et al., 2020; Singh et al., 2020a, c), and these include smart home, energy, education, healthcare, transportation, and business. Other areas of application include military, critical infrastructures, and cybernetics.

IoT forms one of the key components of the smart manufacturing of Industry 4.0 by providing sensing capability and smart connectivity for the CPS that controls and manages production infrastructures and machineries. It also provides real-time monitoring of industrial process to enhance vehicle diagnostic, prevent accident, and speed up production time.

5 Applications of CPS and IoT in Industry 4.0

The literature has documented applications of CPS in manufacturing facility management and monitoring. Liu et al. (2015) established a chaotic forecasting procedure for the time series to overcome the CPS regulation of the chaotic state. A reasoning model architecture as a framework for CPS research proposed by Niggemann et al. (2015) illustrated how data-motivated methods for instance real-time data collection and storing strategies, data processing and machine learning procedures, task-specific HMI, and response/regulator systems can be addressed.

CPS has been introduced to direct the application of autonomous vehicles in smart mobility technology. Hunter et al. (2013) proposed innovative procedures for estimating transportable period disseminations from small, raucous GPS capacities obtained from automobiles on a very huge network in real time. As a substitute to the current manually controlled taxonomy system, Berger (2014) established an automatic methodology for documenting vehicle sensor data in the database.

In addition, CPS has experienced implementation in healthcare administration, especially in customized healthcare systems. Zhang et al. (2015) recommended a cyber physical framework for patient-centered medical treatment software and facilities, called Health-CPS, erected on cloud and large-data analytics machineries.

Together, IoT and CPS has been used to simplify the planning, development, and evaluation of smart cities and buildings. Shih et al. (2016) reviewed IoT/CPS based smart cities and buildings creation and challenges focused on middleware, computing paradigm, fault tolerance, data quality, and virtual run-time setting. Analytical methodology was used to analyze how certain variables in the IoT/CPS environment would affect architecture. Our research found that well-built IoT/CPS would reduce energy usage as well as increase protection in buildings and cities.

In Industry 4.0, several other works have been based on the underlying security risk in the implementation of CPS. Lee et al. (2019) established a Blockchain technology's possible impacts in the creation and implementation of real-world CPPSs. A cohesive three-level Blockchain model was suggested as a business roadmap for specifically defining Blockchain's ability, integrating, improving, and combining this technology into Industry 4.0 development processes. As there are many problems relating to data confidentiality, anonymity, centralization, networking, etc., in CPS that need further growth and improvement, Blockchain-based software has been used to alleviate the underlying real-time deployment concerns of cyber physical structures in the technology realm of manufacture. The suggested coupling is intended to promote coordination and data flow within the current CPS framework to ensure the safe and efficient functioning of the production systems.

6 Integrated IoT-CPS Models for Industry 4.0

Vital industrial tools for instance machineries and material management structures are rendered 'smart' in Industry 4.0 to interpret real-time position, interact and react effectively to manufacturing vicissitudes and turbulences in an independent means based on the convergence of various IoT and CPS technologies. Lu (2017) stated that CPS controls physical processes within Industry 4.0's hierarchical organized smart manufacturing by producing a simulated replica of the real environment and makes autonomous decisions. CPS connects and cooperates with each other and with users in real time over the IoT network, and the Internet of Services (IoS) is delivered and used by value chain members (Lu, 2017). IoT and CPS are designed to help systems that capture and handle massive volumes of sensor-generated data in real-world environments, and CPS also helps them to leverage scarce resources more effectively using data processing and connectivity tools to minimize costs, develop technology, and provide creative and high-quality services. A lot of work has been undertaken to explore the feasibility of combining IoT with CPS to improve the capacity and efficiency of smart manufacturing systems (Ochoa et al., 2017). This section analyzes the various IoT-CPS models or systems introduced and applied in the smart manufacturing literature in Industry 4.0.

Kim and Park (2017) introduced a new approach for improving the production system through the CPS and IoT. Through actively incorporating IoT technology into CPS, a computational model of the cyber physical development system was introduced. Finally, CPS-based IoT architecture was used for linking the physical world and the cyber environment with an emphasis on the manufacturing processes.

Tu et al. (2016) presented an IoT-centered CPS architecture context to enable the incorporation of IoT and CPS, implemented an IoT-centered CPS model built on the architecture context for a production-logistics application as a case study, and devised experimental assessment procedures for IoT-based CPS prototype. The proposed framework as presented in Fig. 7 consists of two parts: the embedded system iNode which is part of the CPS and the IoT cloud which comprises the RFID sensor networks.

The work followed a systematic design method by carrying out emulation experiments and cost-benefit analysis followed by the advancement of architype scheme and testbed platform for the IoT-centered CPS architecture framework. The simulation and investigational assessment of the proposed framework were conducted on the testbed, and the investigational outcomes were evaluated. Experimental discoveries have shown that the proposed integrated approach outperforms the existing barcode-based method in terms of performance, labor costs, and organizational adaptability. The IoT-based CPS system assessment shows major changes in manufacturing logistics activities and decreased component inventory in a rapidly shifting shop floor environment. The study has unlocked innovative paths in manufacturing management and supply chain applications for IoT-built CPS science. This also offered realistic advice for future IoT-based CPS development.

A theory explaining the structure and procedure of smart production-logistics schemes is presented in Zhang et al. (2018) to incorporate smart modeling of vital industrial properties, and to analyze self-establishing arrangement processes for the smart production-logistics network (SPLS). SPLS is developed as a three-layer computational architecture that includes smart models, smart production-logistics frameworks, and self-establishing arrangement layers as depicted in Fig. 8.

The smart design layer combined IoT technologies with sensor network. This layer was built into the CPS and complex action model to represent the real-time state of intelligent resources. Hadoop clusters have been utilized to accumulate and process semi-organized and unorganized data, whereas the data warehouse is utilized for organized data processing. Three aspects were also integrated into this layer: space, functionality, and operation level. The task-driven smart industrial facility chain was implemented in the smart production-logistics network layer for the active reaction, engagement, and collective optimization of SPLS. Cloud computing capabilities encapsulate the manufacturing competency of smart machineries and the logistics competency of smart material management networks such as smart production services and smart logistics services into smart fabrication services.

Within the self-organizing configuration layer, the data is decomposed into manufacturing tasks and logistics tasks until delivery requests or exceptions are reached. Second, the fabrication structure is divided into a three-level ATC pecking order consisting of ATC components. The suggested ATC archetypal is utilized to design industrial tools

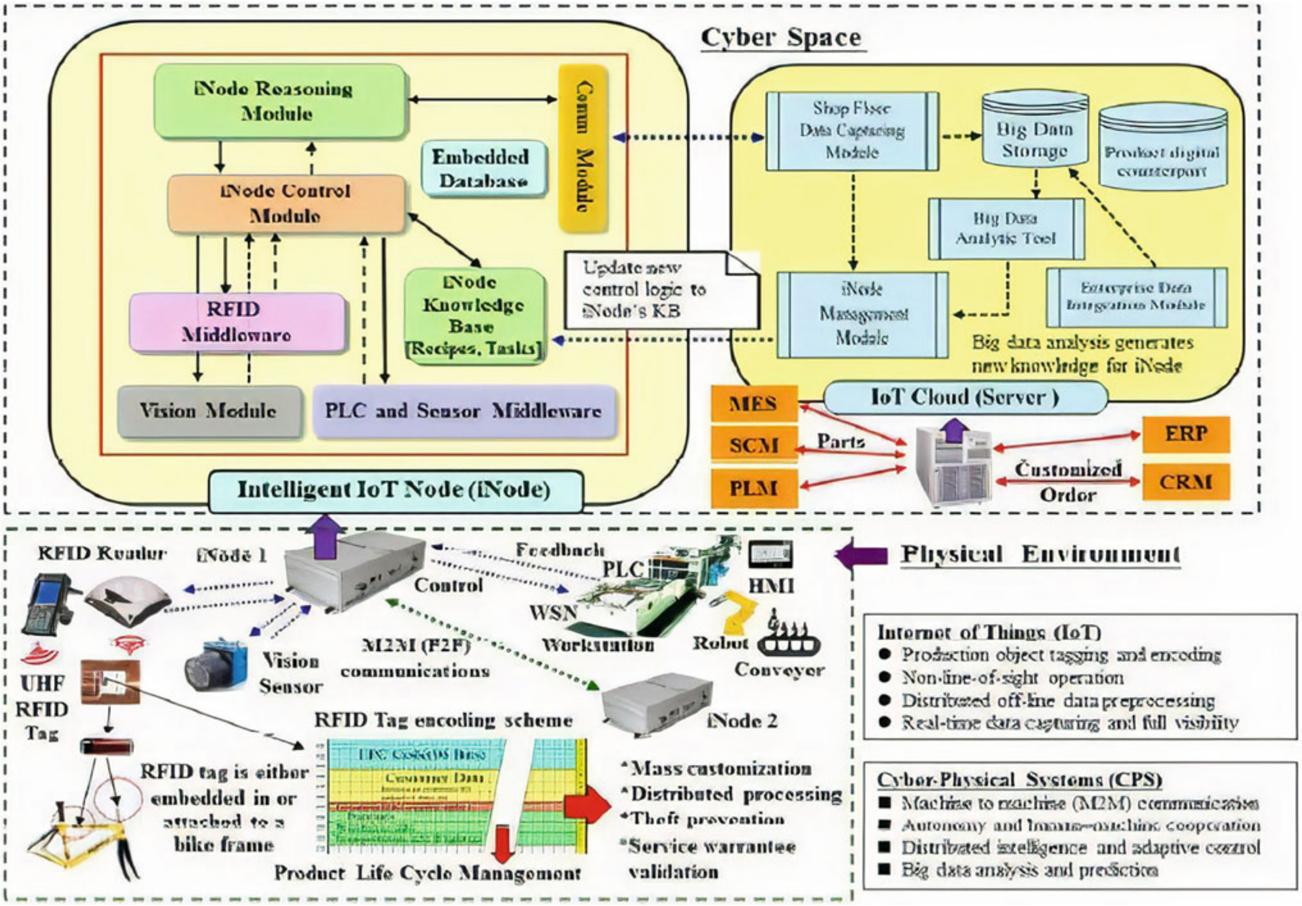


Fig. 7 CPS-IoT framework proposed in (Shih et al., 2016)

like equipment and material management schemes or automobiles conferring to production constraints and the efficiency target such as cost, time, and electricity. The viability of the suggested system was eventually tested, and performance was also assessed using an engine production company. Results showed that processing time and energy usage are decreased, and the estimation period for the suggested method is rational. The work presented theoretically to help manufacturers to implement IoT-CPS related applications and increase production-logistics systems performance.

Tan et al. (2019) presented a DT building structure and scheme for the input of sensor-derived data into a simulation model for an IoT-aided CPS-based development network. DT was implemented independently in three ways, which are mode of integration, mode of measurement, and mode of testing. For modern simulation models, which are mostly utilized for what-if examination and optimization, the test method and investigational approach are usually given. The synchronization approach is a special mode for DT, which distinguishes study mode and experimental mode. The DT continually modifies the simulation model with IoT-derived data.

Through comparing the prototypical production with the real physical outcomes, an interactive procedure amid the factory environment and the simulation modelers validated the DT environment. Upon testing the dependability of the prototypical, the test experiments were running, and the outcomes were evaluated. Findings found that the time interlude established from sensors as contribution from the actual world is precisely similar to the one produced from the cyberspace simulation prototypical. It was verified that the DT simulation harmonization approach could accurately represent the actual conduct of the factory model.

Following the analyzed models, it is clear that the integrated CPS-IoT frameworks can be adopted in smart manufacturing to actualize low cost production, robust production processes, scalable manufacturing, and operational efficiency.

Open Issues in IoT-CPS models

Despite the development and implementation of the IoT-based CPS framework, several issues still remain unresolved. For instance, the effort to associate IoT-built CPS with numerous IoT platforms and corporate

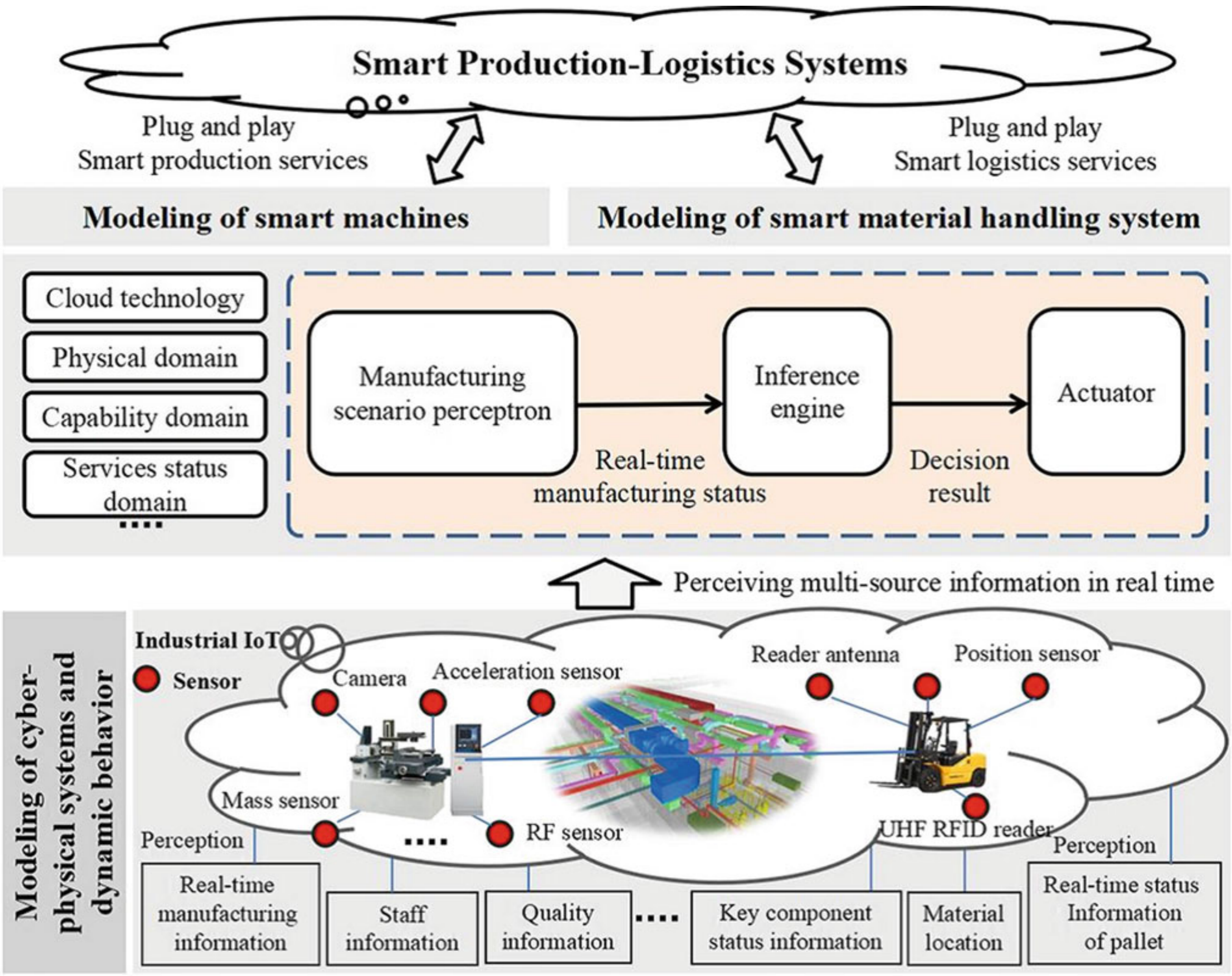


Fig. 8 Layered architecture for smart production-logistic systems (Zhang et al., 2018)

frameworks (e.g., ERP, MES) is still unresolved. New works are needed to bridge this gap between the CPS-IoT frameworks and the existing corporate frameworks.

Another important gray area that require more research is the nonappearance of a norm for M2M communication practice throughout supply chain in the frameworks. More works are needed to design a flexible and robust M2M architectures and protocols that could be seamlessly used within the CPS-IoT frameworks.

Another potential challenge is that in a real-life scenario, the conceptual solutions proposed cannot be entirely implemented due to their complexity. Available solutions have resorted into applying simulation. More works are still needed to empirically implement the proposed frameworks in order to evaluate their effectiveness and efficiency as well as confirm their applicability and suitability.

Moreover, the CPS-IoT frameworks are yet to be extended to several other potential application areas such as emergency services, air travel, vital infrastructure, hospitals and pharmacy, smart transportation, and operation robotics.

7 Conclusion

The emergence of Industry 4.0 has caused a dramatic technological shift in manufacturing industry. Modern manufacturing industry is characterized by intelligent processing, knowledge integration, and adaptability. These characteristic features are provided with the incorporation of CPS and IoT technologies in the manufacturing processes. This chapter discusses the application of CPS and IoT in the advancement of real-world smart manufacturing. It presents the potentials of adopting a unified CPS-IoT framework by factories to transit to Industry 4.0 applications. Various CPS-IoT architectural frameworks are analyzed and reviewed, and lastly open issues in integrated CPS-IoT systems are highlighted. From our analysis, it was discovered that integrated CPS-IOT models have been used widely for production logistics, smart production-logistic network, and optimization of DT building structures. These findings indicated that CPS-IoT frameworks can be adopted in smart manufacturing to achieve robust production processes, low cost production, operational efficiency, and scalable manufacturing. It is, therefore, recommended that the proposed integrated models be extended to other application domains such as critical infrastructure, emergency services, air travel, smart transportation, and operation robotics.

References

Berger, C. (2014). Scenario pattern matching in large sensor recordings with simulation models for cyber-physical systems. In *Proceedings of Society for Computer Simulation International's Summer Simulation Multi-conference* (p. 38).

Böhm, M., Leimeister, S., Ried, C., & Krcmar, H. (2011). Cloud computing—Outsourcing 2.0 or a new business model for IT provisioning? In F. Keuper, C. Oecking, & A. Degenhardt (Eds.), *Proceedings of Application Management* (pp. 31–56). Gabler.

Bordel, B., Alcarria, R., Robles, T., & Martin, D. (2017). Cyber-physical systems: Extending pervasive sensing from control theory to the Internet of Things. *Pervasive and Mobile Computing*. https://doi.org/10.1016/j.pmcj.2017.06.011.

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications, 54,* 1–31. https://doi.org/10.1016/j.comcom.2014.09.008.

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 perspective. *International Journal of Mechanical, Industrial Science and Engineering, 8*(1): 37–44.

Consortium, II. (2019). Industry 4.0 definition industrial internet factsheet. https://www.iiconsortium.org/docs/IIC_FACT_SHEET.pdf.

Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or hype? *IEEE Industrial Electronics Magazine, 8*(2), 56–58.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems, 8*(12), 4242–4268. https://doi.org/10.3837/tiis.2014.12.001.

Hahanov, V. (2018). Cyber physical computing for IoT-driven services. In *Cyber physical computing for IoT-driven services*. https://doi.org/10.1007/978-3-319-54825-8.

Hahanov, V. I., Amer, T. B., Chumachenko, S. V., & Litvinova, E. I. (2015). Qubit technology analysis and diagnosis of digital devices. *Electronic Modeling J, 37*(3), 17–40.

Hehenberger, P., Vogel-Heuser, B., Bradley, D., Eynard, B., Tomiyama, T., & Achiche, S. (2016). Design, modelling, simulation and integration of cyber physical systems: Methods and applications. *Computers in Industry, 82,* 273–289. https://doi.org/10.1016/j.compind.2016.05.006.

Hermann, M., Pentek, T., & Otto, B. (2016). Design principles for industrie 4.0 scenarios. In *Proceedings of the Annual Hawaii International Conference on System Sciences, 2016-March*, (pp. 3928–3937). https://doi.org/10.1109/HICSS.2016.488.

Hunter, T., Das, T., Zaharia, M., Abbeel, P., & Bayen, A. M. (2013). Large-scale estimation incyber physical systems using streaming data: A case study with arterial tra ± c estimation. *IEEE Transactions on Automation Science and Engineering, 10*(4), 884–898.

Hyseni, D., Çiço, B., & Selimi, B. (2016). Conception, design and implementation of an interface for security in cloud controlled by the end user. *International Journal on Information Technologies & Security, 8*(2).

Kagermann, H., & Wahlster, W. (2016). *Industrie 4.0: Smart manufacturing for the future*. Berlin, Germany: Germany Trade and Invest.

Kim, S., & Park, S. (2017). CPS (cyber physical system) based manufacturing system optimization. *Procedia Computer Science, 122,* 518–524. https://doi.org/10.1016/j.procs.2017.11.401.

Kumar, A., & Nayyar, A. (2020). si^3-Industry: A sustainable, intelligent, innovative, internet-of-things industry. In *A roadmap to Industry 4.0: Smart production, sharp business and sustainable development* (pp. 1–21). Cham: Springer.

Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering, 6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4.

Lee, E. A. (2008). Cyber physical systems: Design challenges in object oriented real-time distributed computing. In *11th IEEE International Symposium on Distributed Computing (ISORC)* (pp. 363–369).

Lee, J., Azamfar, M., & Singh, J. (2019). A blockchain enabled cyber-physical system architecture for Industry 4.0 manufacturing systems. *Manufacturing Letters, 20,* 34–39.

Liu, L., Zhao, S., Yu, Z., & Dai, H. (2015). A big data inspired chaotic solution for fuzzy feedback linearization model in cyber-physical systems. *Ad Hoc Networks, 35,* 97–104.

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration, 6*, 1–10. https://doi.org/10.1016/j.jii.2017.04.005.

Marini, A., & Bianchini, D. (2016). Big data as a service for monitoring cyber-physical production systems. In *ECMS*, (pp. 579–586).

Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing* (800–145).

Monostori, L., Kadar, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals-Manufacturing Technology, 65*(2) 621–641 (2016).

Niggemann, O., Biswas, G., Kinnebrew, J. S., Khorasgani, H., Volgmann, S., & Bunte, A. (2015). Data-driven monitoring of cyber-physical systems leveraging on big data and the internet-of-things for diagnosis and control. In *DX@ safe process* (pp. 185–192).

O'donovan, P., Gallagher, C., Bruton, K., & O'Sullivan, D. T. (2018). A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications. *Manufacturing Letters, 15*, 139–142.

Ochoa, S. F., Fortino, G., & Di Fatta, G. (2017). Cyber-physical systems, internet of things and big data. *Future Generation Computer Systems, 75,* 82–84. https://doi.org/10.1016/j.future.2017.05.040.

Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of things technologies for elderly health-care applications. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 217–243). Academic Press.

Ruhse, K. U., & Baturova, M. (2012). Cloud computing: Cloud computing as an integral part of a modern IT strategy. *ISACA Journal, 3,* 6.

Sehgal, A., Agrawal, R., Bhardwaj, R., & Singh, K. K. (2020). Reliability analysis of wireless link for IOT applications under shadow-fading conditions. *Procedia Computer Science, 167,* 1515–1523.

Shih, C. S., Chou, J. J., Reijers, N., & Kuo, T. W. (2016). Designing CPS/IoT applications for smart buildings and cities. *IET Cyber-Physical Systems: Theory & Applications, 1*(1), 3–12. https://doi.org/10.1049/iet-cps.2016.0025.

Singh, A. K., Firoz, N., Tripathi, A., Singh, K. K., Choudhary, P., & Vashist, P. C. (2020a). Internet of things: From hype to reality. In *An industrial IoT approach for pharmaceutical industry growth* (Vol. 2, pp. 191).

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020b). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet, 12*(4), 61.

Singh, M., Sachan, S., Singh, A., & Singh, K. K. (2020c). Internet of things in pharma industry: Possibilities and challenges. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 195–216). Academic Press.

Sztipanovits, J., Koutsoukos, X., Karsai, G., Kottenstette, N., Antsaklis, P., Gupta, V., et al. (2012). Toward a science of cyber-physical system integration. *Proceedings of the IEEE, 100*(1), 29–44.

Tan, Y., Yang, W., Yoshida, K., & Takakuwa, S. (2019). Application of IoT-aided simulation to manufacturing systems in cyber-physical system. *Machines, 7*(1), 2.

Tao, F., Qi, Q., Wang, L. & Nee, A. Y. C. (2019). Digital twins and cyber–physical systems toward smart manufacturing and Industry 4.0: Correlation and comparison. *Engineering, 5*(4), 653–661.

Tu, M. K., Lim, M., & Yang, M. F. (2016). Internet of things-based production logistics and supply chain system-Part 2 : IoT-based cyber-physical system : A framework and evaluation. *Industrial Management & Data Systems*, *118*(1), 96–125. https://doi.org/10.1108/imds-11–2016-0504.

Xu, L. D., & Duan, L. (2019). Big data for cyber physical systems in Industry 4.0: A survey. *Enterprise Information Systems, 13*(2), 148–169.

Zhang, L. (2014). A framework to specify big data driven complex cyber physical control systems. In *Proceedings of IEEE International Conference on Information and Automation (ICIA)*, (Hailar, China, pp. 548–553).

Zhang, L. (2014). Designing big data driven cyber physical systems based on AADL. In *Proceedings of IEEE International Confernce on Systems, Man and Cybernetics (SMC)*, (San Diego, CA, US, pp. 3072–3077).

Zhang, Y., Guo, Z., Lv, J., & Liu, Y. (2018). A framework for smart production-logistics systems based on CPS and industrial IoT. *IEEE Transactions on Industrial Informatics, 14*(9), 4019–4032. https://doi.org/10.1109/TII.2018.2845683.

Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2015a). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal, 11*(1), 88–95.

Zhang, D., Zhao, J., Zhang, F., & He, T. (2015). Urban CPS: A cyber-physical system based on multi-source big infrastructure data for heterogeneous model integration. In *Proceedings ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, (pp. 238–247).

Zheng, P., Sang, Z., Zhong, R. Y., Liu, Y., Liu, C., Mubarok, K., … & Xu, X. (2018). Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering, 13*(2), 137–150.