Smart Security for Industrial and Healthcare IoT Applications

M. Aruna, S. Ananda Kumar, B. Arthi, and Uttam Ghosh

1 Introduction

Internet of Things (IoT) has paved the way for the rapid development of many areas which includes smart transport, smart city, smart home, smart healthcare, etc. Internet applications have become the order of the day, which has grown so rapidly and has become inevitable in almost all human activities [25]. IoT takes the help of various network devices to transfer and exchange data between physical objects which will be connected to each other. The main task of IoT thus becomes remotely regulating these objects throughout an existing network. The IoT device collects the information using the sensors associated with it and transfers it to the server after processing the data if required. The current trend of going for integration between the data processing systems for information and communication technology (ICT) and the medical fields (MF) shows a collective view of nerve connections outside the seam and devices that can improve healthcare services, and anticipate the advent of Internet of Things (IoT) healthcare. The population is growing, and aging is increasing. Diseases worldwide are seeking effective healthcare solutions protecting the health of the people. Another notable improvisation that has become

M. Aruna (✉) · B. Arthi
Department of Computer Science and Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Chennai, TN, India
e-mail: arunam@srmist.edu.in; arthib@srmist.edu.in

S. Ananda Kumar
School of Computer Science Engineering, VIT- University, Vellore, India
e-mail: s.anandakumar@vit.ac.in

U. Ghosh
Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA
e-mail: uttam.ghosh@vanderbilt.edu

U. Ghosh et al. (eds.), *Intelligent Internet of Things for Healthcare and Industry*,
Internet of Things, https://doi.org/10.1007/978-3-030-81473-1_17

a development trend and gain widespread recognition around the world is the smart manufacturing system which is based on cyber-physical manufacturing system (CPMS). The primary advantage of IoT is to simplify human efforts, by intellectual techniques, which also makes inter-device connection smooth and effective in almost all the fields [22].

2 Key Security Goals in IoT

The advantages of IoT technology are many in number when we consider in terms of cost, effectiveness, efficiency, and ease of operation. Like any other advancement in science and technology, IoT also has its own drawbacks and disadvantages when misused. The major drawbacks identified in IoT integrated devices paves a way to many security threats, piracy, and data leaking and causes untold damage to the commercial, political, and social fabrics of a country.

The Internet of Things (IoT) is an inspiring field that combines intellect and intelligence to many essential functionalities of the modern-day world. IoT technology and its features are used in various sectors like homes, hospitals, cities, businesses, construction, and many more. One of the major limitations in the use of IoT and its applications or devices is the privacy and the security threats. This security issues are the main factors that is considered as the hindrance for the widespread use and acceptance of the IoT devices and applications. The storage and processing abilities of the IoT devices and their applications are usually constrained, and the design of these features currently focuses more on guaranteeing functionality and to a large extent ignores other conditions like the security and privacy issues (Fig. 1).

Majority of the security solutions that are currently available requires too many complicated computations and strategies, and hence they are expensive. The traditional security frameworks and algorithms that are currently available are actually very challenging to be implemented for many upcoming IoT devices and its applications or groups of IoT devices. IoT technology requires a flexible, adjustable, and reliable authentication and access control framework to take care of the security and privacy features of the IoT devices and their applications. The conventional access control model that has a centralized work structure cannot support the upcoming or evolving substantial and uncluttered IoT applications and devices. Hence, IoT requires a consistent, adaptable, and trustworthy access control methodology to certify the privacy and security aspects of trivial IoT devices. The traditional access control model has a centralized workflow and arrangement, and hence it is difficult for it to compliment the impending or progressing significant and uncluttered IoT applications and devices.

The lightweight certificateless signature (CLS) system includes niche and edge case scenarios in which there are four types of attacks of signature forgery that CLS fails to address. The first attack is called forgery attack based on public key replacement. Second in line attack is attack from a malicious-but-passive KGC. Third type of attack would be forgery attacks from anyone. The last type of attack

Fig. 1 Key security goals in IoT

such a system is susceptible to is forgery attack from anyone based on any previous messages. Then the paper proposes a robust certificateless system (RCLS). There are several changes made in the generator functions to eliminate the possibility of the first three attacks. The fourth type of attack is eliminated by introducing a partial private key. To achieve higher efficiency, the RCLS scheme is based upon an elliptical curve analogue [18].

The rise of IoT as the fourth industrial revolution can provide a robust and scalable solution to support Industrial Internet of Things (IIoT) by decreasing the load of computational tasks from resource-starved machine-type devices (MTDs) to the high-powered edge servers. The problems of such a system would be the limited spectrum of resources, capacity-constrained batteries, and context unawareness. The proposed model is a learning-based channel selection model which takes into account the three distinct aspects of environmental awareness, namely, the energy consumption awareness, service reliability awareness, and the backlog awareness. The proposed algorithm SEC-MUCB outperforms the regular UCB algorithm by 13.7% and outperforms the range selection algorithm by 31.2%. The paper

concludes with the how MTDs can be utilized just for task offloading as they are fairly limited in their battery capacity. This is only achieved by the power edge computation [20].

3 Industrial Internet of Things (IIoT)

The myriad of trustworthy practices, issues and the application of such in IoT systems. The first point discussed is the idea of a unified IoT trustworthy environment establishment based on edge computing in Industrial IoT (IIoT). Here the threat level to the system depends on the number of IoT devices, and so it is hard if not impossible to counteract it. The machine learning algorithm models that are often trained on sensitive data usually leak the privacy to some form of adversarial attacks, thereby limiting the full potential in Industry 4.0. The work introduces a new approach called PriModChain, a framework that implements constraints for privacy and the trustworthiness on IIoT data by the amalgamation of differential privacy, federated ML, Ethereum blockchain, and smart contracts. The next group of articles discusses the trustworthiness of the system; here it starts with discussing how instrumental damages are done under different specific environmental conditions. Due to this, IIoT would essentially be able to detect system faults through environmental anomalies. The traditional security triad of confidentiality, integrity, and availability still applies to the IIoT, and now privacy must also be included. Finally, the last group of articles discusses the blockchain and its applications in vehicle connectivity [11].

The trustworthiness of a device in the Industrial Internet of Things (IIoT) network is an essential parameter expectation. Maintaining this trustworthiness as a recurring variable for every device in such a network is quite important to avoid loss. A device that is deemed trustworthy in an IIoT system combines the security characteristics of trustworthiness in the information technology sector, i.e., safety, privacy, reliability, security, and resilience. The Ensemble-learning method which combines random subspace (RS) with a random tree (RT) is used for detecting cyberattacks on any SCADA system by using the network traffics as a stream of data based on IIoT platform. A lack of availability of any other efficient and accurate security system for SCADA-based IIoT networks helps to bridge the gap as it satiates both scalability and reliability aspects which aren't present in the already existing systems [15].

With the combination of IoT technology and traditional M2M industry, the Industrial Internet of Things (IIoT) came into being which got the attention from all walks of life. With the increase in the number of IIoT devices in the networks of industrial environments, there is a radical need for research in securing IIoT systems from internal attacks; the threats to the security and quality of service (QoS) issues have skyrocketed. Internal attack is one of the important security issues that has made service environment unsafe and unreliable. Even though there is a lot of IIoT, there is no unified, standardized, and fine-grained system for trust evaluation to

handle the threats of internal attack and improve the overall QoS of IIoT. To this end, there is a need for a standardized model with a unified trustworthy environment which can be achieved by using edge computing which is being proposed; this system can detect malicious service providers and service consumers in a timely fashion, help filter fake data, and recommend the credible service providers. Edge computing is an effective service access point as it can support collection of service records to analyze and perform trust evaluations [17].

3.1 Security Issues in IIoT

Industrial Internet of Things (IIoT) applications aim at the automation industry. Industrial Internet of Things connects sensors, various instruments, and other devices that interact among each other and with computer that support industrial applications, which includes manufacturing, fabrication, and energy management. In the development trend of cyber-physical manufacturing system (CPMS), Industrial Internet of Things (IIoT) is a major issue [26]. Features like mechanization, automation, smart connect, real-time supervising, and cooperative control become the major issues for research and discussion [33].

There is a certain IoT-enabled health and access monitoring service questioning its customers about the location of different regions to optimize their travel in the geographical area. Elevated massive deployment costs of fully reliable information resources include IoT-enabled monitoring services sensing tools for citizen assignation and perhaps unreliable statistics collection for consumers. Nevertheless, trust management becomes a vital factor in the accomplishment of such facilities and services because they can mislead or delude customers through modification or counterfeiting. A hybrid unit or data trust calculation scheme was proposed for the monitoring service which depends on Bayesian practice to score data for users and the Dempster-Shafer theory (DST) for data fusion, only to calculate the reliability of the data. To provide flexibility against developmental change, the likelihood or probability mass used in the DST is updated vigorously relative to the user score above characteristics correlated with registered data [30].

One of the frameworks was proposed that measure the reliability of all data in the presence of on-off attacks. It was validated using massive simulation trials for uniform and on-off attacks. The trust scores differ under different system factors such as attack size and misdiagnosis. In addition, the reliability of all data can be measured using the utility theory and compared the results obtained by probability theory. The probability theory improves the reliability of all data compared to the correct utility theory [29].

The Social Internet of Things (SIoT) is an example of IoT devices that are networked, and they interact and evolve with each other. Social networks are interactions between them and their users. The influence of social relationships between devices and consumers depends on customers and their IoT services equipment. In this structure, evaluation of customer loyalty along with IoT devices is

necessary to prevent malevolent entities from spreading maliciously content or avoid the interruption of the network. One way to estimate companies the credibility for crowdsource companies is to deliver comment or feedback about the collaboration with certain IoT devices and users. Still, privacy protection in the form of crowd-sourcing is a challenge as collaborative responses reveal communication devices and consumer behavior [32]. To deal with this issue, new privacy-protection system was proposed which assesses the reliability of IoT devices and users together in the SIoT ecosystem. This system implements a homomorphic encryption system which supports decentralization, self-implementation, and privacy protection. This ensures that the system is appropriate in computing, privacy, and consumer protection and detects the presence of malicious parties and a combination of consumers [31].

The Internet of Things is popular in all disciplines and in applications of smart construction, smart transport, health, and defense. One of the dimensions of IoT is the socialization of "things" called as Social Internet of Things (SIoT). There is a strong example that connects the principles of IoT and social networking, where the things involved are not only just autonomous and intelligent, but it also includes the social consciousness. A trust management plan was proposed to enable reliable automated decision-making built on the behaviors of objects. The popular SIoT trust metrics used are protection, significance, society interest, etc. Cooperative service scores are used to calculate the reliability power [27].

The distributive nature of IoT networks insists the need to design the appropriate security measures to assist in the detection of maleficent internal nodes. In earlier days the most extensive studies inferred that the attacks were considered primarily by single invasion, but the modern intruder may have more harmful effects since they perform multiple attacks simultaneously or in collaboration. One solution identified was using mix-attack models that have three types of attacks: attack, drop attack, and replay attack. A Distributed Consent Based Trust (DCONST) model was also proposed which utilizes both to assist in assessing the compliance of nodes and to identify bad IoT nodes and malicious individuals [28].

3.1.1 Security Issues in IIoT Based on Blockchain

One of the major challenges in the Internet of Things (IoT) environment is maintaining data integrity and legitimacy of data sources. To guarantee data security, the conventional access control methods and frameworks that are available are not appropriate or adaptable for direct access control in IoT systems due to its complex access management schemes and absence of integrity. Hence, for secured and reliable IoT and IIoT, blockchain is one of the evolutionary approaches. It is a decentralized approach that aims at the security features of IIoT. Blockchain can be considered as a distributed ledger since all its blocks are chained together. It can track and coordinate transactions and save information for the billions of devices in the IoT. Blockchain is another important subject that is constantly evolving among the technology and the entrepreneurial society. Blockchain is a freely accessible,

visible, and distributed record that tracks all transactions between two groups very effectively which can be traceable, and which is permanent.

Blockchain is the primary security tool that is required for IoT systems. The combination of blockchain, fog computing, edge computing, and IoT devices are becoming extremely popular and useful. Incentive and feedback mechanisms are discussed as further enhancement for the system. The base blockchain is then compared to this enhanced blockchain where strength and weakness of both are compared in a tabular form. Then the author discusses wearable IoT devices; here the layers and the model for healthcare are discussed first, and then issues regarding security and privacy are discussed next. In AWS platform, the components of the API that enables IoT acts as a gateway for devices, message brokering, and rule operation engine. Finally the paper is concluded with referencing a suggestion made to AWSACIoT and the need for standardization in IoT's data collection and data sharing [2].

Blockchain technology acts as a framework for multimedia data processing. Its role is to ensure the privacy and transparency of any patient's records, ease of document accessibility and the shipment process among provider and customer. Blockchain phenomenon requires a web-based application consisting of two ends such as the front end that connects with the patients and a back end that facilitates patients to acquire the data from the blockchain. The miner's task here in blockchain is to provide proof of validation for correct task order. Even if the patient changes their doctor, the information regarding previous tests and medicines remain in the blockchain. The MAC layer protocol used is 802.11, and transmission ranges of MAP routers are 120 m/s. This type of system helps in computing the trust and rating of the nodes after a specific interval of time [10].

An efficient blockchain-assisted secure device authentication mechanism BASA IIoT is required to solve the problem of cross-domain internal communication among the IoT nodes while assessing and keeping the rising threat levels under check. Specifically, the consortium blockchain is primarily introduced to facilitate the construction of trust among several differential domains. The most exploited form of data authentication during the authentication process is identity-based signature (IBS); in order to preserve the privacy of devices, we need an identity management mechanism, which can comprehend that devices being authentic persist unknown. Besides, session keys between two parties are negotiated, which can secure the subsequent cross-domain internal communications. The limitations of BASA are the increased power consumption and the increase in communication overhead [12].

The differential privacy (DP) policy model achieves high records of privacy by maximizing the likelihood of the individual record identification. Other option is PriModChain; here there are two major components, namely, distributed entity (DISTEN) and central authority (CENTAUTH), which ensure the trustworthiness in terms of privacy, security, reliability, safety, and resilience of the IIoT system. DISTEN's task is to extract model parameters, whereas CENTAUTH applies multi-encryption key on the global parameters of the IPVC. Basically CENTAUTH first retrieves the encrypted IPFS hashes of the encrypted local (DISTEN) model

parameters that are released within the federation interval. PriModChain generates excellent results toward trustworthy privacy preserving in IIoT systems, and it reduces latency to improve efficiency [13].

The importance of Industrial Internet of Things (IIoT) lies in security as it is susceptible to a lot of single-point attacks and malicious attacks, which cannot in turn provide stable services. Due to the robustness and security brought by blockchain, this proposition about combining the security and stability of blockchain with the scalability of IoT has gained a considerable amount of traction. The major issue is that blockchains are power-intensive and low-throughput, making them unsuitable for a lot of power-constrained IoT devices. To combat these challenges, a blockchain system that is based on credit consensus mechanism for a network of IIoT devices is required. A credit-based proof-of-work (PoW) algorithm is the primary verification mechanism and a data authority management method for IIoT devices since it ensures security and transaction efficiency of the system at the same time and protects sensitive data confidentiality, which would regulate the accessibility to sensor data [16].

The fundamental problems affecting both IIoT and blockchain technology are interoperability, scalability, portability, and security. A platform-agnostic tokenizer for blockchain of IIoT devices referred to as Industrial Blockchain Tokenizer (IBT) helps with the tasks of data exchange in IIoT networks. This acquired data is then processed on a local system to get fruitful edge filtering results. This technology can bridge the gap between IoT and blockchain as well as result in standardization in both of them using IBT which can self-compute both cryptographic and networking operations leaving only the IIoT sensors and assets to do their job [19].

3.2 Industry 4.0

Industrial Internet of Things (IIoT) system is capable of realizing Industry 4.0 features of the industry that are normally assembled into operational and information technology (OT, IT) in order to promote technologies concepts, tools, and methods, which will enhance efficiency, flexibility, sustainability, and quality of life with reduced costs. Figure 2 shows Industry 4.0 architecture.

Each IIoT system and Industry 4.0 have the following requirement such as business, function, information, communication, integration, and asset concerns:

- Domain logic of the business is mapped to capture the grouped distribution of business across the IIoT device hierarchy and business logic and leads to understanding of the infrastructure and functional requirements of the business.
- To decompose the business capabilities into functional requirements using domain knowledge across the networked IIoT systems using service interfaces.
- The data, its meaning, and format are captured in information view.

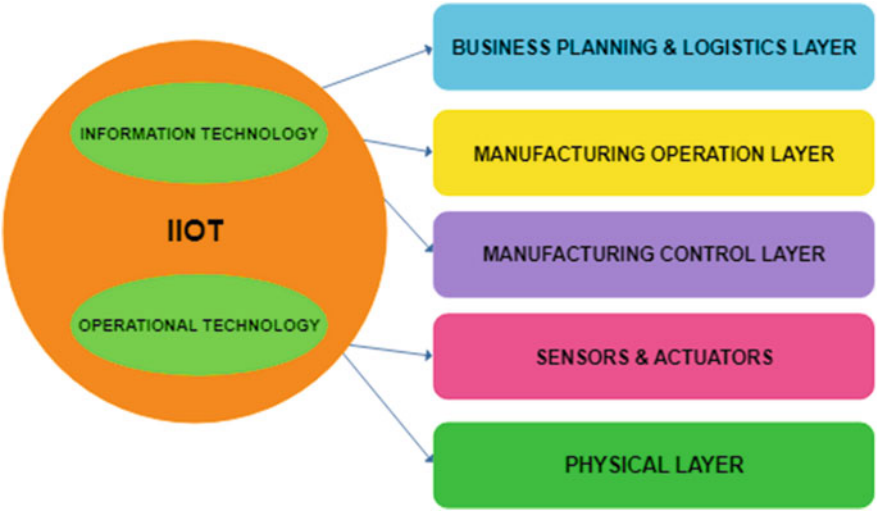

Fig. 2 Architecture of Industry 4.0

- Information passed between systems must be serialized/de-serialized, compressed/decompressed, and encrypted/decrypted and are captured using communications view.
- In integration view, hardware interfaces used in the systems for interacting with the physical world are captured.
- To identify the essential devices for running, the systems are captured in asset view since legacy devices are highly distributed in IIoT systems.

The system view can be used for development and estimation of the system and captures the asset, integration, communication, information, function, and business in terms of an implementation view. Table 1 shows various attacks and threats [9] [14] found in IIoT devices.

3.3 5G-Enabled IIoT

One revolutionary technology that is changing the appearance and work structure of the industries in a very smart way is the Industrial Internet of Things (IIoT). IIoT can be considered as one of the evolutionary applications in IoT in the field of industry and automation field. Although IIoT has many advantages and opportunities, it equally has many challenges and threats. IIoT connects sensors, actuators, computers, and many more that makes the manufacturing procedures extremely effective and smart. To accomplish the objective of "Internet of Everything (IoE)," cell network with wide inclusion has continuously become a strongly significant transporter of IIoT.

Table 1 IIoT attacks and threats

	IIoT devices	Attacks	Threats
Operational technology	Sensors Actuators Motors Transmitters Embedded devices	• Malware • Injecting input • Eavesdropping • Brute-force attacks	• Failure/malfunction of sensor/actuator • Device theft • Vandalism and sabotage • Man-in-the-middle attack • Session hijacking
	Gateways Distributed control systems PLCs	• Wireless device attacks • Replay attack • Man-in-the-middle attack • Sniffing • Brute-force password guessing	• Failure/malfunction of a control system • IoT communication protocol hijacking • Communication network outage • Network reconnaissance • Power supply outage • Loss of support services
	SCADA control Operator stations Control room	• Malwares • IP spoofing • Data sniffing and manipulation	• Unintentional change of data • Change in configuration of OT system • Erroneous use of devices • Maladministration systems • Third party's damage to system
Information technology	Data centers Office application Web services	• Web application attacks • Phishing • SQL injections • DNS poisoning	• Manipulation of hardware & software, information • Denial of service • Malware and targeted attacks • Abuse of personal data • Brute-force attacks
	Mobile devices Internet Business applications Data analytics	• Mobile device attacks • DoS and man-in-the-middle attacks • Side-channel attacks • Authentication attacks • Cloud malware • Injection	• Failure or disruption of service providers • Failure to meet contractual requirements • Violation of rules and regulations • Breach of legislation

The fifth-generation cell network (5G) which is happening is required to be a binding together organization that will associate billions of devices to help various business situations. But, as the industry needs, demands, and the number of the connected devices are growing tremendously, the conventional cloud-based IIoT framework is not efficient to handle it. The upcoming 5G era, which uses mobile edge computing (MEC) to improvise the 5G supporting IIoT, binds together organization that will associate many of devices to help various business situations. This type of architecture is normally data oriented. As indicated by the necessities of the IIoT application, the data structure and the data flow graph and the relating information structure are planned to start from the top.

Based on the fixed data plane, the information interaction is performed between the device and the application. It is easy to be implemented in small and simple

IoT requirements (e.g., smart homes). With the increase in the devices to be connected and the business requirements, the frame will not be suitable for an IIoT applications. With the advent of "Internet of Thing," the cloud-based architecture requirement of IIoT is difficult to satisfy the requirements such as intensive computing, low latency, high reliability, and large connections. Considering this constrain, using MEC in IIoT applications has gained acceptance. However, it has been noted that mainstream MEC framework has limitation in providing the required support for the IIoT. Hence, a novel IIoT-MEC architectural framework was proposed which consists of three layers, namely, cloud computing layer, IIoT-MEC layer, and device layer.

In this new framework IIoT-MEC, the resource blocks in MEC servers are sliced into numerous resource blocks using Docker containers. Using the virtualization concept, the hardware details of the diverse IIoT devices are shielded using some resource blocks for device function virtualization. This simplifies the development of IIoT into a simple software development. With the resource block being used to support the IIoT operation services efficiently, a flexible object-oriented architecture is developed. The development of IIoT-MEC is done using Linux system, python language, and Docker container which makes the system highly compatible and minimizes the hardware requirement. This enables the IIoT-MEC to seamlessly integrate with any open-source platforms and work on low-cost machines like Raspberry Pi and PC.

4 IIoT in Healthcare

A unique framework model for the future IoT-based healthcare systems, which can be used for both standard programs and programs that assess specific situations, is proposed. Neutral sensors acts as a strong force on patient for recognizing important symptoms, blood pressure, and blood oxygen-levels. Communication rates are short and long; they are then compared according to appropriate healthcare applications. BLE and NB-IoT have emerged as the most appropriate standards of short width and long length in health, respectively. On analyzing some of the state-of-the-art tech in the new sensory fields, communication standards, and cloud technology, few key areas for some much-needed future research can be identified and analyzed. Machine learning and development of a secure systems are potentially strong in offering a solution to the researchers who want to make a big difference in IoT based health field [21].

The current trend of integrating the data processing systems for information and communication technology (ICT) and the medical fields (MF) shows a collective view of nerve connections outside the seam and devices that can help in improving healthcare services, and anticipating the advent of Internet of Things (IoT) healthcare. This provides relevant guidance for IoT health service developers, starting with the user's view of technology. In particular, the authors suggest potential risks impact on users' access to IoT lifecycle management service. Details on

professional service providers, scope of work, devices, professional support, and shared lists of personal medical information were suggested as important attributes. Friendship analysis is calculated by measuring the equal value of suggested symbols and service description options. The study can be performed by collecting the medical information and medical history from many respondents, analyzing the data and model, and then comparing the power groups with distinct medical history. The results have shown that the prospective users, basically, need a reliable, secured, harmless, and safe health service. This model has a great potential, while medical history has had a profound effect on what is known the significance of the proposed symbols.

As the population is rising enormously and the aging is increasing, diseases worldwide are seeking effective healthcare solutions protecting the health of the people. IoT healthcare monitoring applications can help reduce stress on healthcare systems and for healthcare providers, thus reducing and improving healthcare costs. Homecare and particularly elderly patients with persistent disease can be majorly benefitted from this. Healthcare sector and IoT Tiered Architecture (IoTTA) proposed a policy to change sensor data in real-time clinical responses. This methodology examines several features including sensing, sending, processing, storage, and mining learning. This framework is useful and aids in the development of effective steps to continue system enhancement in IoT healthcare applications. The growth of some IoT applications has huge implications for the healthcare industry as concerning to fields such as self-care, data mining, and machine learning [23].

Figure 3 depicts the various applications of IoT in healthcare. As the recognition of the Internet of Things (IoT) devices and additional remote patient monitoring systems increases, the security issues related to these devices also increase. About data transfer and logging of transactions, to maintain protected health information (PHI) blockchain-based smart contracts can be used to enable reliable analysis and maintenance of the medical sensor. To write the records of all events in the blockchain, a private blockchain which is based on an Ethereum protocol is used. This blockchain is used to build a system with sensors that communicate with a smart device called smart agreement. This smart agreement approach helps in medical field for real-time patient monitoring and medical intervention by sending reports to patients and medical experts, who also have a protected record of carrying out these activities. It helps fix the multiple issues with security and major real-time vulnerabilities associated with the use of remote patient examining and automatic distribution of information to all participated parties in a HIPAA-compliant manner [24].

The current IoT healthcare data integration semantic techniques include wearable body area network (WBAN), body area network (BAN), intelligent medical sensor (IMS), and personal monitoring device (PMD). The ontologies such as Resource Description Framework (RDF) and its schema are discussed. Then other technologies like Web Ontology Language (OWL) and semantic techniques like Simple Protocol and RDF Query Language (SPARQL) are also discussed. One of the techniques for data integration is clustering, and then distribution-based

Fig. 3 Applications of IoT in healthcare

mechanisms are used, as being good with synthetic data that forms distinctly sized clusters but has a poor exception handling. The other technique is centroid based model which is fast and accurate, but moderately useless if the number of clusters is unknown or data is too large [1].

A new protocol for IoT healthcare communication, WBAN, is implanted in the body, and all the sensors are connected to a body coordinator (BC). This BC can be supplemented with external power unlike the sensor nodules. All the sensors are connected to this BC in star topology. Next, the pape discusses the traffic taxonomy, for example, emergency traffic, delay-constrained traffic, reliability-constrained traffic, and normal traffic. Then the ThMAC proposition is further lined. The primary component of this model is modeling thermal rise; here an equation is given to find out the temperature of point x,y as at any given time. A superframe is the second component to ThMAC; here beacon-enabled mode is followed. The next component is thermal-aware wake-up schedule; here the communication cycles of sensors within the superframe are discussed. Fourth component is the MAC operations carried out under ThMAC during a superframe; here contention access periods, polling periods, DL periods, CFP periods, and emergency data management are discussed. ThMAC is then tested in a simulated environment. This

is measured by maximum rise in temperature metric. The paper concludes with ThMAC outperforming IEEE 802.15.6 in achieving lower average temperatures and energy efficiency [3].

The fundamentals of IoT-based solutions in assisted ambient living (AAL), relies on the framework of semantic message-oriented middleware (SeMoM) architecture. After this the model being proposed is discussed; the discussion starts with laying down the methodology of the model. Any anomalies in the AAL system are traced and sent to a symptom indicator (SI); this stream of symptoms is then analyzed to figure out the disease. If multiple instances of similar disease are observed in close vicinity, an epidemic is detected. There is a SeMoM extension here added to the system. The ADL component is responsible for sensors and their ontology, SI component acts as a publisher of SI streams, and finally the disease component acts as a recipient of these streams from SI. A scalable semantic framework is proposed for disease and epidemic monitoring in a compound of elderly. This framework would have a significant effect in improving safety and aging in place for elderly as long as they desire staying at home. The power of this newly proposed system comes from the scalability and precision required to facilitate required results in detection of epidemics [4].

Figure 4 represents the various advantages of using IoT in healthcare applications. The security concern for user-generated data (UGD) is done through digital real-time consent which involves data collection for medical research. This is explored further, in which the data rights of the users is investigated deeper into the trust management aspect of IoT. Identification of trustworthy and untrustworthy parties is explored as well. The Health Insurance Portability and Accountability Act (HIPAA) is concerned about data privacy rights of the consumers, and data quality parameters include accuracy, authenticity, confidentiality, freshness, availability, and integrity. The basic three principles in the framework are the following: data should only be collected and used by trusted and certified entities with consent, data collection should be done in real time, and proper cryptographic mechanisms must be employed for the purpose of data protection. The privacy-preserving participants' selection methodology is required for user data consent and data monetization to encourage use participation. The framework combines all of the prior-mentioned components into one model for standardization in healthcare IoT [5].

IoT architecture of healthcare systems and its primary applications has a lot of challenges and also potential opportunities among which cloud integration and its components and the role of big data in IoT are considered primary. After establishing the components of IoT healthcare system, the shortcomings of each of these components are discussed. The first point of contention is as IoT devices are used all over the body and for extended period of time, the comfort levels of such devices need to be assessed. The next problem is that of noise removal in digital signal in real time. Removing human supervision with multiple agent machine learning algorithms checking, tracking, and determining the appropriate actions is not only cost-effective but also yields higher accuracy levels. The next point of contention is energy consumption and requirement of better energy optimization algorithms. The next problem mentioned is that of storage, where vast amounts of

Fig. 4 Advantages of using of IoT in healthcare

data points are stored, but this storage needs to be easy access. Lastly the paper explores the area of privacy regarding IoT devices. The IoT healthcare architecture provides effective monitoring of the elderly patients by using a camera, speaker, and sensors that improves scalability and reliability [6].

Smart remote monitoring in real-time operations requires ease of access and transmittance of decisions based on acquiring data that includes data handling, data consent, data acquisition, and instrumentation and measurements. Due to the alteration of potential difference in cells, bio-signals such as ECG, EMG, EEG, and EOG are extremely low in amplitude. The signals that have such low amplitude can use bio-amplifiers, and that have low bandwidth and are prone to noise can use bio-compatible electrodes. Safety and isolation circuitry and special measurements are required since bio-signals are activated from different parts of the body. The procedures of data digitization, noise filtering, event identification, and extraction of data done in order to improve the interaction of various small and seemingly unrelated changes result in emergence of a healthcare system model where there is a vast integrated, ubiquitous, and holistic network that can be further supplemented [7].

The current ECG monitor system is low power, has higher processing speeds, and interfaces with multiple communication platforms, but the developed Telecare-ECG IoT device can be used to provide healthcare facilities to patient's home where the equipment can be operated even by nonspecialist users, with limited power supply sources, or used in industrial areas for out-of-hospital cardiac patients who operates daily for acquiring and processing of physiological parameters of the patients. There is a proposition for patients with highly optimized and specialized medical services [8].

5 Conclusion

A deep study on security issues in IoT, Industrial IoT, and its applications and the healthcare in IoT has been carried out. This chapter concludes with various security issues in IoT and IIoT and its applications and healthcare applications. The performance of security challenges is varying for the IoT-based applications. The extensive security issues are studied for IoT healthcare applications, and for industrial applications. This study focuses on the basic and emerging technology of IoT trust issues and various methods of Industrial IoT, Industry 4.0, and 5G-enabled IIoT also for various applications of IoT in healthcare. IoT will be creating a new generation of society enabled with information and knowledge. The application of IoT is unlimited due to advancement in technologies and the ease of integrating multiple devices and components, especially in the consumer sector where most of the homes appliances and systems are now integrated with the smart phones. This advancement has led to the requirement of different technologies to support such integrations. The future of IoT depends on having highly portable technologies which can work on different requirements.

References

1. S. Balakrishna, M. Thirumaran, V.K. Solanki, IoT sensor data integration in healthcare using semantics and machine learning approaches, in *A Handbook of Internet of Things in Biomedical and Cyber-Physical System*, (Springer, Cham, 2020), pp. 275–300
2. M. Tawalbeh, M. Quwaider, A.T. Lo'ai, Authorization model for IoT healthcare systems: Case study, in *2020 11th International Conference on Information and Communication Systems (ICICS)*, (IEEE, 2020), pp. 337–342
3. M.M. Monowar, M.O. Alassafi, On the Design of Thermal-Aware Duty-Cycle MAC protocol for IoT healthcare. Sensors **20**(5), 1243 (2020)
4. R. Zgheib, S. Kristiansen, E. Conchon, T. Plageman, V. Goebel, R. Bastide, A scalable semantic framework for IoT healthcare applications. J. Ambient. Intell. Humaniz. Comput., 1–19 (2020)
5. M.J.M. Chowdhury, A. S. M. Kayes, P. Watters, P. Scolyer-Gray, A. Ng. Patient controlled, privacy preserving IoT healthcare data sharing framework. in *Proceedings of the 53rd Hawaii International Conference on System Sciences*. (2020)
6. S. Selvaraj, S. Sundaravaradhan, Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl. Sci. **2**(1), 139 (2020)
7. A.S.M.S. Arefin, K.M.T. Nahiyan, M. Rabbani, The basics of healthcare IoT: Data acquisition, medical devices, instrumentations and measurements, in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, (Springer, Cham, 2020), pp. 1–37
8. I. Zagan, V.G. Găitan, A.-I. Petrariu, N. Iuga, A. Brezulianu, Design, fabrication, and testing of an IoT healthcare cardiac monitoring device. Computers **9**(1), 15 (2020)
9. V. Sklyar, V. Kharchenko, ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios. in *The 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, (Metz, France, 2019), pp. 1046–1049
10. G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimed. Tools Appl., 1–23 (2019)

11. M.Z.A. Bhuiyan, S.-Y. Kuo, J. Cao, G. Wang, Trustworthiness in industrial IoT systems and applications. IEEE Trans. Industr Inform (2020)
12. M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, D. Xiaojiang, M. Guizani, Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J. Sel. Areas Commun. **38**(5), 942–954 (2020)
13. P.C.M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, M. Atiquzzaman, A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Trans. Industr. Inform. **16**(9), 6092–6102 (2020)
14. A.C. Panchal, V.M. Khadse, P.N. Mahalle Security issues in IIoT: a comprehensive survey of attacks on IIoT and its countermeasures. in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 124–130
15. M.M. Hassan, A. Gumaei, S. Huda, A. Almogren, Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model. IEEE Trans. Industr Inform **16**(9), 6154–6162 (2020)
16. J. Huang, L. Kong, G. Chen, M.-Y. Wu, L. Xue, P. Zeng, Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Trans. Industr. Inform. **15**(6), 3680–3689 (2019)
17. T. Wang, W. Pan, S. Cai, Y. Ma, A. Liu, M. Xie, A unified trustworthy environment establishment based on edge computing in industrial IoT. IEEE Trans. Industr Inform **16**(9), 6083–6091 (2019)
18. Y. Zhang, R.H. Deng, Z. Dong, J. Li, P. Wu, J. Cao, Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. IEEE Trans Industr Inform **15**(9), 5099–5108 (2019)
19. D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi, L. Ricci, L. Rizzello, A Blockchain tokenizer for industrial IOT trustless applications. Futur. Gener. Comput. Syst. **105**, 432–445 (2020)
20. H. Liao, Z. Zhou, X.W. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, S.H. Ahmed, A.K. Bashir, Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT. IEEE Internet Things J. **7**(5), 4260–4277 (2019)
21. S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access **5**, 26521–26544 (2017)
22. S. Kim, S. Kim, User preference for an IoT healthcare application for lifestyle disease management. Telecommun. Policy **42**(4), 304–314 (2018)
23. H. H. Nguyen, F. Mirza, M. A. Naeem, M. Nguyen. A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback. in *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, (IEEE, 2017), pp. 257–262
24. K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 130 (2018)
25. B. Oryema, H.-S. Kim, W. Li, J.T. Park. Design and implementation of an interoperable messaging system for IoT healthcare services. in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, (IEEE, 2017), pp. 45–52
26. J. Cheng, W. Chen, F. Tao, C.-L. Lin, Industrial IoT in 5G environment towards smart manufacturing. J. Ind. Inf. Integr. **10**, 10–19 (2018)
27. A.M. Kowshalya, M.L. Valarmathi, Trust management for reliable decision making among social objects in the social Internet of things. IET Netw **6**(4), 75–80 (2017)
28. Z. Ma, L. Liang, W. Meng, Towards multiple-mix-attack detection via consensus-based trust management in IoT networks. Comput. Secur. **101898** (2020)
29. M. Salimitari, S. Bhattacharjee, M. Chatterjee, Y.P. Fallah, A Prospect theoretic approach for trust management in IoT networks under manipulation attacks. ACM Trans. Sens. Netw. (TOSN) **16**(3), 1–26 (2020)
30. B. Shayesteh, V. Hakami, A. Akbari, A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. Int. J. Inf. Secur. **19**(1), 93–110 (2020)

31. M.A. Azad, S. Bag, F. Hao, A. Shalaginov, Decentralized self-enforcing trust management system for social Internet of things. IEEE Internet Things J. **7**(4), 2690–2703 (2020)
32. G. Srivastava, S. Muneeswari, R. Venkataraman, V. Kavitha, N. Parthiban, A review of the state of the art in business intelligence software. Enterp. Inform. Syst. (2021). https://doi.org/10.1080/17517575.2021.1872107
33. U. Ghosh, P. Chatterjee, R. Datta, A.Pathan, Secure Addressing Protocols for Mobile Ad hoc Networks. in *Security Analytics for Internet of Everything*, (CRC Press, Boca Raton, 2019)

Dr. M. Aruna holds a Ph.D. degree in the Faculty of Information and Communication Engineering from Anna University, Chennai, India. She has 15+ years of experience in teaching. Her area of interest includes artificial intelligence, machine learning, IoT, cloud computing, and software engineering. She has published several articles in various reputed journals. She has also published a book chapter in CRC Press. She is an active reviewer of various journals. She has presented papers in various national and international conferences and attended many workshops, seminars, and faculty development programs to be in track with the changing technology and teaching methodology. She is a member of various scientific and professional bodies.

Dr. S. Anandakumar holds a Ph.D. degree in the field of computer science from VIT University. He possesses one decade of experience in teaching and worked as project assistant in IIT Kharagpur. His areas of interest include QoS in wireless sensor networks, green computing, mobile computing, ad hoc networks, MANET, data mining, and IoT. He has published numerous articles in Scopus and SCI-indexed journals. He presented his articles in various national and international conferences and attended many faculty developments programs in order to keep pace with changing teaching environment. He is a member of various scientific and professional bodies. Apart from teaching he is passionate about social services and rural development activities.

Dr. B. Arthi holds a Ph.D. degree in the field of computer science and engineering from Anna University. She has 15+ years of experience in teaching. Her areas of interest include software engineering, IoT, cloud computing, and green computing. She has published several articles in various reputed journals. She has also published a book chapter in CRC Press. She has presented papers in various national and international conferences and attended many workshops, seminars, and faculty development programs to be in track with the changing technology and teaching methodology. She is a member of various scientific and professional bodies. She has been awarded the IET Inspiring Young Teacher Award for the year 2016–2017 for the IET Chennai.

Dr. Uttam Ghosh joined Vanderbilt University as an assistant professor of the practice of electrical engineering and computer science in January 2018. He obtained his Ph.D. in electronics and electrical engineering from the Indian Institute of Technology Kharagpur, India, in 2013, and has postdoctoral experience at the University of Illinois in Urbana-Champaign, Fordham University, and Tennessee State University. His main research interests include cybersecurity, computer networks, wireless networks, information-centric networking, and software-defined networking. Dr. Ghosh is selected for Junior Faculty Teaching Fellow for 2018–2019 in Vanderbilt University. He is also serving as associate editor and reviewers of reputed journals and conferences. He is a senior member of the IEEE and member of Sigma Xi, AAAS, ASEE, and ACM.