Chapter 6
Privacy and Security Concerns in IoT-Based Healthcare Systems

Joseph Bamidele Awotunde, Rasheed Gbenga Jimoh, Sakinat Oluwabukonla Folorunso, Emmanuel Abidemi Adeniyi, Kazeem Moses Abiodun, and Oluwatobi Oluwaseyi Banjo

6.1 Introduction

In recent years, the healthcare system and technology have been deeply entangled. As the outcome of fast-paced growth in the areas of the Internet of Things (IoT), new opportunities are now arising. Furthermore, with the adoption of wearable biosensors by the people across the globe, there are newly emerged applications for individualized telemedicine and mobile health. This new emergence of these technologies is a result of their high availability, simplicity to personalize, and easy accessibility, thus enabling the providers to deliver personalized content cost-effectively on large scale easily. Also, big data analytics and IoT are progressively gaining more attraction for the next generation of mHealth and eHealth facilities. Despite the new fields evolving rapidly, they also have their shortcomings, particularly when the goal is healthcare systems with a complicated problem, difficult in energy-efficient, safe, flexible, suitable, and consistent solutions. More especially when it comes to the issue of security and privacy of IoT generally. It has been projected that IoT will rise to a market scope of $300B by 2022 in healthcare covering the medical devices, systems, applications, and services sectors [1].

J. B. Awotunde (✉) · R. G. Jimoh
Department of Computer Science, University of Ilorin, Ilorin, Nigeria
e-mail: awotunde.jb@unilorin.edu.ng; jimoh_rasheed@unilorin.edu.ng

S. O. Folorunso · O. O. Banjo
Department of Mathematical Science, Olabisi Onabanjo University, Ago-Iwoye, Nigeria
e-mail: sakinat.folorunso@oouagoiwoye.edu.ng; banjo.tobi@oouagoiwoye.edu.ng

E. A. Adeniyi · K. M. Abiodun
Department of Computer Science, Landmark University, Omu Aran, Nigeria
e-mail: adeniyi.emmanuel@lmu.edu.ng; moses.abiodun@lmu.edu.ng

P. Siarry et al. (eds.), *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*, Internet of Things,
https://doi.org/10.1007/978-3-030-75220-0_6

IoT allows a broad range of intelligent applications and resources to solve the problems facing individuals or the healthcare sector [2]. For instance, P to D (Patient-to-Doctor), P to M (Patient to Machine), S to M (Sensor to Mobile), M to H (Mobile to Human), D to M (Device to Machine), O to O (Object to Object), D to M (Doctor to Machine), and T to R (Tag to Reader) have dynamic IoT link capabilities. This brings people, computers, smart devices, and complex systems together intelligently to ensure a productive healthcare system [3, 4]. The healthcare system that depends on IoT assists the individuals and aid their vital everyday life activities. Remote patient monitoring is one such technology, common for the diagnosis, treatment, and care of patients.

These IoT devices connect to cloud infrastructures such as Google Cloud Computing, Microsoft Azure Cloud, Amazon Web Services, or any other custom web services capturing storage and analytics information. Furthermore, IoT services include remote medical observation of persons with chronic or long-term situations. These systems can monitor elderly patient treatment instructions and track the position of patients who are placed on wearable healthcare tools in hospitals and clinics. The collected health information can then be delivered to their care provider. Medical devices that can be integrated or deployed as IoT technology are infusion pumps that attach to analytical dashboards and hospital beds with sensors that measure the vital signs of patients. The IoT receives its maximum capabilities through the use of objects, i.e., "Smart" objects, which use multiple sensors and actuators fully prepared to learn in their context, and through the use of embedded communication infrastructure to communicate with any possible alternatives; it is not enough to collect a huge of data alone, and it must be turned to use materials that can help organizations to revolutionize their business processes.

While IoT has produced extraordinary prospects that aid in increasing income, decrease costs, and improve efficiencies, it is very important to put all the huge amounts of data into use. Enterprises need to build a network where a large amount of sensor data can be processed, handled, and analyzed robustly and cost-effectively way to generate benefits from IoT [5]. In this context, it is important to use a big data tool that can help ingest and read different data sources as well as facilitate the process of data integration. Integration and review of data allow businesses to revolutionize their business processes. In particular, these companies may transform a huge sum of money of sensor-collected data on valuable observation using data analytics software.

The IoT systems not only monitoring patients health status in real-time but can also be used to mining information collected from patients through IoT devices. The sensor-fitted devices are most data collection tools in the IoT setting that require data distribution service and message queue telemetry transport called custom protocols. The IoT sensors are expected to produce an immense volume of data because these devices are almost found in all fields. The data created from IoT objects can be used to investigate the impact of any events or decisions, treatment, diagnosis, prediction of any illness, and finding potential research trends. The generated data are processed using different data analytic tools [6].

In the field of healthcare, IoT devices such as satellites could have diverse applications, such as heart beat monitoring, blood sugar level monitoring, and capsule endoscopy [7]. The combination of sensors and actuators, as well as other mobile technology equipment, will transform the medical industry's functioning especially during any infectious disease outbreak [8]. Such systems, known as the Internet of Medical Things (IoMT), are a coupled structure of healthcare smart devices that receive information subsequently offered by web communications systems to healthcare IT systems [9, 10]. Currently, 3.7 million therapeutic equipment is already in practice then linked to and monitored by different portions of the body to notify medical resolutions [11].

Cloud computing enables businesses to easily handle enormous data and extract valuable data from the collected data, which are the fundamental obstacles facing big data technologies. To ensure the consistency of the software, the cloud offers enormous space for data storage and processing. However, cloud storage is impacted by the number of leaks and outflows. The structure should be built to protect data secrecy. To avoid data theft by unauthorized users, encryption methods might be more useful [12]. To make the system more autonomous and effective, the decentralized techniques should include different data and research division. This improves the precision of analysis that ensures a stable data-cloud platform. In the cloud-based world, protection is the main challenge and new technology can develop to guarantee data security and privacy in the cloud environment [13].

These IoT devices connect to cloud infrastructures such as Google Public Computing, Microsoft Azure Cloud, Amazon Web Services, or any other custom web services capturing storage and analytics information. Furthermore, IoT services include remote medical observation of persons with chronic or long-term situations. These systems can monitor elderly patient treatment instructions and track the position of patients who are placed on wearable healthcare tools in hospitals and clinics.

The use of IoT in monitoring patient healthcare using sensors and devices comes with tremendous security concerns. The recent sophisticated attacks like data integrity, data breaching, and data collusion are major safety and confidentiality concerns of IoT in IoT-based healthcare monitoring systems. During data communication of patients' health monitoring data, there are conventional solutions presented. But they are unable to deal with complex attacks at the period of data transfer and fail to fight the recent attacks on IoT-based healthcare system. The safety of data collected from IoT sensors and devices such as blood glucose, body temperature, fetal monitors, and ECG are crucial to patient's lives. Hence, it has become paramount for the IoT community, computer experts, and healthcare providers to secure each sensor/device in the IoT environment with the integrity of its data that will guarantee the device's security and privacy.

The safety and security of IoT devices are greatly affected by cyber-attacks and threats, yet the protection and comfort of the daily health of patients depend on this data gathering. Also, the privacy of patients' sensitive data can be affected. Popular forms of attacks in healthcare are ransomware, DDoS attacks, insider, email breach, and deceit scams [14]. Besides, there are other types of communication attacks such

as data credibility, data breach, eavesdropping, impersonation, and conspiracy, among others. Specifically, these security and privacy of the new threats/attacks pose problems, such that the data may be breached during data communication [15], thus making patient personal data to be exposed. Similar conditions preclude the awareness of patents in the future of IoT healthcare because these issues are not treated in a timely and proper manner.

Although there are numerous security protocols, like encryption and other security implementations, MAC techniques, public-key cryptography, k-anonymity, and many more [16–20], to secure data from threats/attacks. When relating them to IoT-based health systems, they also have distinctive boundaries in terms of processor enactment, energy cost, device cost, etc. While many current works provide data privacy protection over contact to patients, when a cloud service has been agreed upon, they do not protect the data, particularly when a cloud service is under threat by an insider or service vendor. The IoT model also needs appropriate clarifications to safeguard patient information from Internet threats/strikes from sensing devices to healthcare providers. This study consequently discusses the issues of privacy and security in IoT healthcare systems and provides an overview of IoT, including its architectural design. This chapter also suggested a framework to secure healthcare information in the IoT environment.

The rest of this chapter is prearranged as follows: Section 6.2 discusses the overview of the Internet of Things. Section 6.3 presents the Internet of Things solution for the healthcare system. Section 6.4 presents the security and privacy of the Internet of Things in healthcare applications. Section 6.5 presents the architecture for the secure transmission of healthcare information in an IoT-based environment. Lastly, Section 6.6 concludes the chapter and discusses future works for the realization of efficient uses of the framework in healthcare systems.

6.2 Overview of Internet of Things

The rapid merging and technological expansions of micro-electro-mechanical digital electronics and wireless communication technologies resulted in the advent of IoT Internet of Things. The IoT has given birth to the recent growth in the number of sensors and devices connected, and an increase in the data collected from these devices is called big data. The consumption reflects how the evolution of big data naturally overlays with IoT-based devices. These give upsurge to non-trivial worries about processing data, data analysis, security, and the managing of big data in an uninterruptedly escalating system [21]. The scientists have studied the issues connected with the effective utilization of IoT to address these concerns. The convergence of these has created several opportunities despite different studies on big data, analytics, and IoT for the flourishing of big data and analytics in IoT systems [21].

The report from Cisco has it that the quantity of items coupled through the Internet has passed the number of human beings globally [22, 23]. Internet-connected gadgets that make up IoT networks include laptops, PCs, tablets,

Fig. 6.1 Internet of Things with different devices

WiFi-enabled detectors, wearable devices, medical instruments, and home appliances, among others, as seen in Fig. 6.1. According to estimates, the volume of Internet-connected users is projected to increase from 22.9 billion in 2016 to 50 billion by 2020 [24].

6.2.1 The Physical Objects IoT-Based Components

The concepts of IoT include a collection of technologies that allow a broad variety of devices and objects to use networking technologies to link, communicate, and interact. The initial solution for the implementation of the IoT-based systems is the radio-frequency identification (RFID) technology. The IoT-based wearable devices have proved to be cost-effective and have been promoted in recent years in sensing technologies. The idea of customized IoT-based healthcare systems has been introduced and is becoming increasingly popular. The use of a series of interconnected devices has been used by patients to create an IoT network dedicated to healthcare evaluation in healthcare networks system. Physical artifacts (also known as physical

devices): In these contexts, they capture, classify, and monitor information. This involves machines that track the vital signs of a patient (body temperature, heart rate, blood glucose, blood pressure, everyday life). Physical devices are linked to the Internet and turn the physical world's patient-related information into digital data. Physical artifacts are used in their environments to gather, track, classify, and provide data about patient physiological effects. In an IoT-based framework, objects are very important as data cannot be captured and obtained from the patient without them.

Sensors are responsible for defining items and collecting information from cameras, identifiers, and others. Production of low-cost and small-scale embedded devices such as wearable devices (e.g., accelerators, gyroscopes or barometric pressure sensors) and physiological sensors (e.g., spirometers, skin temperature sensors, or blood pressure monitors) as well as wearable devices (e.g., exercise bands or cell phones) has enabled the process of measuring and sounding characteristics of individuals. GPS localization and Bluetooth, among others are built into the devices. Several researchers are exploring regular wearable tracking sensors for physical inactivity being a major risk factor in the healthcare system.

For the monitoring of dynamic activities, an accelerometer is widely used. For difference among the standing, sitting, or lying, an accelerometer needs to be placed on a specific part of the body [25] and by setting a threshold and value for discrimination [26]. In measuring rotational movements, gyroscope devices are usually used as an extra tool. The detection of behaviors like [27], is measured by calculating the angular speed of movement of the patient, such as bent knees, descending stairs [28], ascending stairs [29], or turning [30]. A barometric measuring device, including an accelerometer, is also useful for monitoring the activity of the stairs [31] and fall detection [32]. Wearable devices are also goods for wristbands that monitor the number of steps, distance, and calories burned. Such wearable devices communicate through Bluetooth with a mobile phone using relevant mobile applications. Smartwatches and cell phones are now substitutes for traditional sensors that are portable.

6.3 Internet of Things Solutions for Healthcare Systems

Although the IoT-enabled healthcare system technologies are still at an early stage, potential industry applications are rapidly emerging and increasing. Many healthcare-enabled research projects and industrial cases relevant to IoT have been developed and deployed.

IoT-based frameworks will simplify healthcare procedures and increase the efficiency of patient care by allowing various organizations to cooperate [33]. In specific, Ambient-assisted living aims to ease the daily lives of people with disabilities and serious health conditions. Many ground-breaking services can be provided by the use of IoT in this field, such as the gathering of critical health

information through a sensor network, the transfer of data to a cloud medical facility for storing and analysis, and the effective regulation of sensor data [8, 33].

A significant advantage of the IoT Healthcare system's incorporation is that it delivers low-cost and ubiquitous health services of high quality. A large quantity of sensor network information that needs to be handled for additional data processing is created by pervasive healthcare systems [34, 35]. This represents a solution for the efficient management of patient medical data collected through the sensor network and enables the abstraction of technical information, removing the need for technological infrastructure expertise [22, 24]. Besides, it results in the simple computerization of the data collection and distribution process at a cheap cost. It would also allow mobile devices suitable for entry, distribution, retrieval, and communication of health information [36].

By improving the protection of therapeutic data and the accessibility and redundancy of resources, Cloud enables this application scenario to face common challenges such as safety, secrecy, and consistency. It is essential to provide live-assisted facilities in real time due to the efficient operation of sensor data [37]. The IoT-based cloud also allows the safe execution of cloud-based multimedia-based health services, which can solve the problem of running large multimedia on some devices with limited computing and low battery capabilities. It also offers a versatile storage and management technology for streaming data generated in healthcare body sensor networks, both online and offline. The wearable monitoring systems can be implemented in a group of people due to the use of the IoT Health model and can produce vast quantities of contextual data that are collected, processed, and analyzed in a scalable manner [38, 39]. The use of IoT technology in healthcare systems has several advantages, and the resulting services can be separated into categories for monitoring individuals (e.g., patients and staff) and artifacts, patient recognition, and authentication, sensing, and automated collection of data in sensor networks.

6.3.1 Categories of IoT Applications in Healthcare Systems

Self-management services in telemonitoring and AAL settings have become a heated facial study and implementation point in recent years, designed to meet the particular demand of the patients to increase the effectiveness and performance of a treatment (e.g., adjusting the dosage of the patient). The processes offer an alternative approach to improving patients' quality of life (QoL) through contact between patients, doctors, and caregivers. These systems can deal with a range of patient situations using sensor technology, objective and subjective methods of diagnosis, care plans, and recommendations, providing patients with personalized information and guidance based on their input. When gathering and storing appropriate health data, the "Closed Loop Principle" is the practice of the service and then transmitting feedback to the patient [40].

Healthcare Monitoring System

In current wearable fitness applications, heart rate monitors, ECG monitors, glucose monitoring, pulse oximeters, and blood pressure monitors are used. Micro- and nanochemical sensors are planned to be complemented shortly to include a continuous medical diagnosis. Additional chemical signals, e.g., in air and sweat, which can be translated into medical surveillance (e.g., people with asthma, other cardiovascular conditions, skin infections, and pharmacokinetics of drugs) can be identified by these miniaturized smart sensors.

Monitoring is the environment where IoT devices and applications have been used to track patient health status and overall well-being. Examples include assisted living in the environment, active aging, therapy and entertainment, contact and social events, health status tracking, diet, and body weight. Community control, enhancing the quality of life, and encouraging living comfortably and independently are the key goals of this group of applications. Monitoring is the most common application field for many individuals and encourages healthy and independent living. It is the most common example of methods of tracking aged care [41]. It has been noticed that the elderly tended to sit at home and to accept technologies if it helps them to live independently [42]. One prominent use in this section is Ambient-Assisted Living (AAL), which is a term used to track and enable aged people to live peacefully and conveniently. AAL systems track the everyday activities of the patient to recognize abnormal circumstances and emergencies and facilitate the daily life of the patient. AAL can enhance both the patient and the caregiver's quality of life by doing so.

IoT applications for tracking and helping patients with severe disorders such as diabetes mellitus and cardiovascular diseases are included in this field. In the implementation of home-based clinical screening services for aged people with chronic conditions, these applications can be extended to disabilities who want to preserve their independent lifestyle [43]. For elderly villages or homes, this could be a perfect solution as it could support the simultaneous monitoring of many individuals [44]. It is suggested that the use of remote monitoring can not only minimize the rate of mortality and hospital referral and admittance, but also be efficient in the treatment of infectious diseases. An example of this is a smartphone program named MAHI, which can collect Bluetooth glucometer blood glucose data and post data on the web for recommendations to the caregiver [45]. Besides, once elderly mental health conditions became persistent, such as stress and anxiety, long-term data could be detected by evaluating small behavioral improvements [46].

Node Physical Characteristics

Different characteristics may be needed for the sensor and devices involved: type factor, height, weight, and energy usage; flexibility and ergonomic criteria; a degree of IP & IK protection, battery capacity; Internet access; processing and location

prerequisites; multimodality and range of interaction; performance and latency limitations; self-healing and EMC criteria; and implementation cost.

Recognition of Human Activity

Human Behavior Identification (HAR) and Tracking of the everyday life of the elderly is another essential feature. The device can detect abnormal circumstances by constantly tracking the behaviors of elderly people and can decrease the effects of unexpected events such as sudden falls [47]. To avoid straying, HAR may also identify the position of the aged and the availability of communication aid. The positioning of artifacts will support the aged people to quickly locate their personal and household objects [48].

Clinical Applications

Inpatient healthcare, IoT clinical applications include disease detection and diagnostics, prediction of disease, and treatment. A more accurate diagnosis and efficient treatment of several diseases [49] can be provided by technology. The device can detect seizures and alert the patient, for example, and send warnings to caregivers [45]. Telehealth and its sub-categories, like teleconsultation and telediagnosis, give specialist consultation by communication devices to patients who are unable to come to medical centers [50].

Preventive Measures

The IoT will track and avoid the occurrence of such harmful conditions. In older patients with chronic disease, for example, the risk of contracting pressure ulcers is high, which can lead to lifelong illness, and the patients may die from ulcers [51]. The use of pressure sensors to recognize the pressure points of older patients based on different positions and to prevent the development of pressure ulcers will solve this kind of issue. Also, pressure distribution data for elderly people with chronic diseases can be used in the design of mattresses and wheelchairs [52].

Mental Health

IoT technology is used to track, anticipate, and take care of elderly patients' mental disorders [46]. It has been mentioned that by analyzing changes in everyday activities in long term surveillance, several forms of mental health disorders could be observed or even predicted. A common field in this application category is dementia. Technology is used in these systems to support people with dementia or other mental illnesses. For instance, by mitigating anxiety, promoting a positive

disposition, and minimizing isolation, an intelligent robot is quite beneficial as a companion to older people with dementia [53, 54]. This lets them have a social life that is more involved.

Rehabilitation

The use of wearable devices can promote many facets of recovery facilities, such as providing input to patients and health workers, or measuring the efficacy of the rehabilitation process [55], or supporting incapacitated patients. Sharma et al. [54, 56] noted that elderly adults and stroke patients would benefit from autonomous exoskeletons of the hip joint, which can support individuals during recovery.

Accessibility to Healthcare Facilities

Mobile health innovations can be used to offer patients living in hard-to-reach areas with quicker healthcare facilities [57]. Besides, older persons can acquire a lot about health knowledge and advancement programs [58], allowing certain disease problems to be self-managed. In patients with osteoarthritis of the knee, the use of pedometer driven exercise guidance from a study in self-management was shown to be more successful than health education alone [59].

Accessibility for Caregivers

Together with smartphones, wearable technology enables healthcare professionals to provide real-time monitoring and treatment for patients remotely [45, 54]. Physicians can access the patient's health data and provide input through a web browser. To recognize emergencies such as falls, elevated heart rate, and send warnings to the caregiver as well as the emergency center, the mobile may also be programmed [45].

6.4 IoT Healthcare Protection and Privacy Technologies

The major problems facing today's healthcare systems include population aging, the prevalence of chronic illnesses, the shortage of healthcare professionals, and the unpredictable growth in healthcare costs, among other factors. Public and private sector actors should work to solve these challenges and find more innovative and accessible solutions that can be applied in out-of-hospital settings. Recent technological developments have greatly changed the understanding of an individual's conventional way of conducting day-to-day operations. In the real world, including the healthcare background, the Internet of Things has to be a rising trend in different

segments. This rapid IoT revolution, however, has also generated some uncertainties and concerns about the protection of data that is stored in different connected items. If the number of items such as sensors and computers increases, it becomes more difficult to maintain robust protection and the privacy of sensitive data.

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

To enhance the comfort of patients concerning the protection and secrecy dangers they pose to the lives of patients and other effects, such as privacy breaches and financial threats, safe and protected IoT healthcare applications are needed. Through reviewing the components of the technology platform in-depth, this chapter focuses on privacy and security challenges in IoT healthcare systems.

Remote patient management processes and warning systems are assisted by health care providers and applications. Data are the most valuable asset of these applications as knowledge obtained through these processes is known to be vulnerable [60, 61].

Besides, it is important to ensure the confidentiality and availability of such data. Sensitive data should be protected, as should protect against unlawful entry, other challenges, and risks. Conversely, due to the amount of data provided by the wearable sensors and the constant interaction between the devices in the system [60], these are difficult areas in the IoT ecosystem. Healthcare practitioners and software developers have worked together in recent years to create stable IoT healthcare applications to solve these problems [61].

Also, the inherent difficulties impede the services offered by IoT technology. The problems often prevent patients from implementing smart healthcare systems, taking into account the problems posed by privacy and security issues [62]. In a device concerned with confidential data, trust is also a crucial factor. Therefore, it would increase the performance of the programs and loyalty between clients by creating a layout that addresses the entire threat landscape. As a result, IoT healthcare will encourage more individuals to benefit from it [60].

6.4.1 Security Concern in IoT Healthcare Applications

In a wide variation of healthcare applications, the IoT plays an important role, from chronic disease treatment at one end of the continuum to disease prevention at the other end. This involves gathering physiological data using sensors, analyzing and archiving the information using gateway devices and the cloud, and then wirelessly sending the scrutinized data to healthcare authorities for additional study and evaluation [63]. Not only can these applications enhance access to treatment while increasing the quality of care, but they will also decrease the cost of care. Publishing new technology without considering protection in healthcare applications leaves patient privacy vulnerable; a person's physiological data are highly sensitive.

Modern healthcare would need ubiquitous health tracking with the least real contact between doctors and patients, which can be accomplished by the IoT definition. Wearable, implantable, or wearable wireless medical sensors can be combined with different forms of wireless communication motes (such as Mica2, MicaZ, Telos, etc.) [64]. Such wireless medical sensors have gathered/generated large quantities of information that must be protected from security attacks. When transmitting to remote locations, we can escape several malicious data attacks by implementing protection algorithms/techniques [65]. Security is also a primary prerequisite for healthcare applications. For ethical and legal purposes, the effectiveness of healthcare applications depends primarily on patient protection and privacy [63, 65].

However, in terms of information safety and confidentiality, the sum of related gadgets and the huge sum of impressionable datasets gathered by those gadgets have brought novel challenges. Cyber-attacks have also changed along with the rapid development of IoT and had created a recent avenue of invasion and risk to the whole medical industry. Many studies explored IoT's numerous privacy and protection issues and device weaknesses in cloud and fog computing settings relevant to IoT-based medical management gadgets [66, 67] and [66] analyzed the IoMT protection and confidentiality taxonomy in detail.

The safety and confidentiality of records relating to patients are twofold essential notions. When we refer to record safety, this signifies that records are securely stowed and transmitted to ensure their absoluteness, genuineness, and legitimacy. Record confidentiality signifies that records can solitary be obtained by individuals who are authorized to sight and utilized it [68, 69]. More rational security measures may be established with different objectives and specifications in mind. The extensive utilization of IoT gadgets offers an improved assurance of an individual's health [70], but it also places a great deal of demand on record safety and concealment.

Consequently, efficacious IoT advancement needs to accept safety and confidentiality as an essential concentration. Although most healthcare establishments don't devote sufficient funds to shield safety and confidentiality [68], there isn't any hesitation that safety and confidentiality perform a significant function in IoT. IoT gadgets create a growing amount of ever more complex real-time records, which is extremely delicate. On one side, the failure of health

organization or system security may have catastrophic consequences. On the other hand, privacy information for the patient is accessible at all levels of record processing, record transfer, cloud storage, and record republication.

Since IoT gadgets don't possess enough reminiscence, computation, and information transmission abilities, they need an efficient, accessible high-performance computation and a large storage system for real-time computation and record stowage. Several IoT organizations currently deposit the health records collected and extend their application servers into the cloud. The apps will get their medical activities uploaded into the cloud appropriately. Cloud facilities enable a hopeful clarification for the effectual administration of ubiquitous medical records through their resistance and capacity to obtain public resources and mutual infrastructure in a pervasive and universal manner.

The diversity of IoT components makes the security concerns of IoT applications more complex for users. Thus, it is the main concern for the production of these IoT applications to recognize and deal with these security problems. Confidentiality, integrity, and availability (CIA) can be summarized as the minimum security criteria for the applications.

Security Issues for Communication Technologies

Security risks and connectivity technologies problems in IoT-based healthcare networks come in several forms. For instance, the activation of DoS/DDoS attacks, comprising of flood attacks, black hole attacks, and home attacks, is a safety problem for these technologies [4]. These systems are also susceptible to secure coupling, interface, usability, power usage, and exploration mode switching on/off, leveraging main ex-change function, baritone loss, identity fraud, monitoring, surveillance, suspicious activities, and linkage interference [71]. Intrusion 27 to track suspicious activations, identity-based authentication, anti-jamming, and packet filtering to block unauthorized users from accessing are the security strategies that should be implemented in this community. The encryption of all wireless traffic often guarantees that the data transmitted through wireless networks are confidential. Also, to prevent the alteration of communications, strong authentication is necessary.

Trusted Third-Party Auditing

The information from sensors may somehow be skewed at sources though appear right during transmission, or intentionally changed by malware by an unauthorized user in the IoT system through the Internet. These distorted data could then be used to make decisions on life and death. Hence, trusting the data provided to us may be questionable, and the issue is yet to be handle properly. Compassionate therapy is linked to another form of trust. Caring is about the relationship between the patient, their families and community, nurses, and other health providers, one that is being

forged. Compassionate care for the sick is a duty for all healthcare providers, but kindness depends on trust.

Nursing, for instance, has been ranked as the most truthful, ethical career for the 14th straight year [72]. This high rating was based on a relationship with patients and the public that starts with confidence and a personal connection. Besides, technology has helped to transform health care by enabling better diagnosis, surveillance, and treatment. Nurses must incorporate technologies at many levels with the implementation of IoT in healthcare and decide about the right use for their practice and how to use technology to achieve better patient outcomes. The same would have to be done by other healthcare practitioners.

Cloud servers aren't completely reliable. Where data manipulation, as well as erasure, occurs lacking consumer authorization, the quality and accuracy of healthcare records deposited in the cloud may be in jeopardy. The data standards are usually particularized by the consumer for security reasons so that the server supplier isn't in an undeviating connection with the record basis. Furthermore, the reputable trusted third party (TTP), which delivers the impartial audit outcomes, could be properly presented to allow cloud service providers to be accountable and to shield the authentic advantages of cloud operators [68]. Trusted third party inspects to enhance security in cloud storage. The TTP's work a wireless transmission issues consist of complex audits, batch auditing, and performance measurement auditing.

Data Anonymization

Clinician-delicate information can be divided into three categories: specific identifiers, quasi-identifiers, and privacy attributes. An explicit identification, such as an ID number, name, and mobile phone number, may be used to identify a patient distinctly. An amalgamation of quasi-identifiers may also provide a specific indication of a patient, such as age, birth information, and address. Privacy information ascribes to a patient's delicate characteristics, which includes sickness and profits. While considering the allocation features of the earliest data in the procedure of data publication, it's crucial to guarantee that the personal characteristics of the novel dataset are accurately treated to assure the confidentiality of the patient.

Currently, haphazardperturbation expertise and anonymous data technology are typically utilized to resolve such issues as k-anonymity, l-diversity, and confidence bounding. The conventional k-anonymity is particularly extensively utilized. The disadvantage, however, is that it doesn't restrict delicate records, and invaders may utilize steadiness invasion and contextual information invasion to recognize delicate information and individual communication, resulting in privacy loss [68].

Security and privacy for IoT devices remain huge issues that bring a whole new degree of user privacy concerns online. This is because such apps can only collect personal information, such as the names of users and telephone numbers, but cannot also track user behaviors (e.g., when users are in their homes and what they had at lunchtime). It is therefore very important to build an IoT based on security and privacy to ensure trust and privacy for users during the use of IoT.

Security Issues for Application

Several organizations have widely accepted IoT and big data analytics. These pieces of machinery are, however, yet in their first phases. It has not yet tackled several current work challenges. Big data analysis is a crucial dispute for several utilizations owing to the nature of data and the scalability of fundamental procedures that support these methods [73, 74]. This segment thus poses some difficulties in the big data analytics focused on IoT.

Data security concerns occur where a network is corrupted by the utilization of big data analytics techniques to infer or reestablish individual information, while data are created by anonymous users. The confidentiality matter has to turn out to be a central concern in the data mining province with the advent of big data analytics tools employed in IoT. Consequently, most consumers are hesitant to rely on such networks, which do not have firm terms of service-level agreement (SLA) concerning abuse or misuse of personal information by customers. Users' sensitive information must be undisclosed and safeguarded from outside intrusion.

Although provisional identity, concealment, and encryption offer numerous means to implement data protection, ethical considerations, for instance, what to employ, how to utilize, and why employ engendered big data in IoT, must be determined [75]. Alternative safety jeopardy connected with IoT data is the variety of system kinds employed and the complexity of data produced, for instance, fresh computers, data formats, and procedures for communication. These systems are intended to interact with supportive utilization and can have various extents and forms external to the system. Therefore, to authenticate these devices, each unit should be issued by an IoT system with a non-repudiable identification scheme. Besides, organizations will sustain a meta-archive of these related tools for analyzing consideration. This composite architecture of IoT is innovative to safekeeping experts, resulting in elevated security risks. Any intrusion in this case thus violates network stability and disconnects interconnected equipment.

Security and privacy are crucial problems in the collection and storing of vast volumes of data in the setting of IoT-based Big Data Analytics. Similarly, these schemes depend seriously on third party facilities and infrastructure to conduct critical processes and host secluded data. Therefore, unprecedented growth in data volume causes difficulties in obtaining every single part of vital data. There are no long-standing security mechanisms that provide full security in IoT-based Big Data scenarios [76–78]. Current algorithms are not meant for complex data interpretation and are thus not implemented effectually. Legacy data protection approaches are primarily designed for static datasets, while the actual data specifications dynamically alter [76, 79, 80]. Therefore, it is difficult to deploy these safety resolutions for energetically cumulative data.

Data Search

Sensitivedata must be scrambled before contracting out to preserve data confidentiality, which obsolescence the current use of data built on readable keyword searches. Allowing an encoded record pursuit service in the cloud is thus of utmost significance. The main approaches for searchable encryption comprise searchable symmetric encryption (SSE) and keyword search public-key encryption (PEKS). It should also be remembered that the further sophisticated the encryption methods, the easier it is to scan the data, and the easier it is to verify the accuracy of the search results. If the results of the search cannot be enforced appropriately, then all protection and privacy safeguards have less value [68].

Access Control

Access control is the way an information scheme determines an individual's uniqueness and predefined rules that prohibit unauthorized individuals from retrieving resources [68]. Access control involves various encryption methods, such as private key encryption (PKE), public-key encryption (PKE), and attribute-based encryption (ABE) [68].

Security Issues for Physical Objects

Physical entity vulnerability concerns include

Physical attacks: The majority of IoT computers, such as constrained utility nodes, are small and wirelessly connected. Thus, it is essential to protect confidential data held in IoT devices and provide IoT-related safe storage resources. There seems to be an elevated risk of threats since more data are believed to be in flow than in traditional architectures and unintended access to data transmitted [81, 82]. On the other hand, the edge technology layer can be defined as an intermediate layer that each has its safety specifications [83].

IntegratingRFIDinto IoT: In IoT applications for users, RFID technology has been used for identifying, tracking, and tracing disabled users. However, because of resource limitations, RFID systems are vulnerable to being targeted. The RFID system, virtualization system, and the Internet are the three basic components of the IoT-based RFID systems [84]. Numerous securities refer to modules such as eavesdropping, middle attack, denial of service, spoofing, copying, monitoring, tag misuse, and wireless connectivity threats. [85]. That's why we ought to secure and restrict access to RFID tag information. To avoid peer-to-peer eavesdropping [86]. As RFID technology does not involve a line of sight, if it is not encoded, unauthorized RFID readers can obtain the data. In addition, by using elliptic curve cryptography [87], authentication in IoT applications based on RFID is enhanced.

IntegratingWSNsinto IoT: There are minimal computing and energy resources in those technologies. They are operated by batteries, and via lossy connections, they are linked. They are still fragile enough to be targeted by any rival. An intruder can install malicious nodes that can operate together to inflict harm to the system. Another problem is how a sensor node and an Internet host can protect the channel [88]. WSNs have been used for healthcare in many delicate IoT systems, so if WSNs protection is attacked, it can result in human harm and loss of resources [89]. Therefore, such security requirements for WSNs must be taken into accounts, such as the encryption and measurement for data confidentiality and integrity of the Message Authentication Code (MAC), security protocols for a safe location, and accessibility.

Denial of Service (DoS) attacks: DoS attacks on IoT systems are the most common and simplest attacks to introduce. They can be seen in many ways and are defined as an attack that can compromise the ability of the network or systems to perform anticipated functions. The IoT has been widely criticized since its conception for the lack of attention given to safety concerns in the design and implementation of its hardware, software, and infrastructure components. This negligent approach has led to numerous vulnerabilities that have already been successfully exploited by hackers and cybercriminals to compromise IoT elements so that they can be misused for different purposes, including the staging of Denial of Service and DoS threats [90]. DoS attacks and DoS (DDoS) sharing allow network facilities/data inaccessible for users. When DoS attacks have been compromised by various nodes, it is known as a DDoS attack. Despite their often sophisticated and commercially appealing exterior design, many IoT devices are built from cheap generic hardware components. These chips and firmware usually contain security vulnerabilities that are essentially built-in and thus difficult for owners and operators to track. Also, the infrastructure and coordination of firmware and software updates for the wireless problem are still at a primitive level. So, it is also hard to update or repair these unsecured IoT computers.

6.4.2 Privacy Issues in IoT Healthcare Applications

The most critical problem is data privacy in the IoT. The patient's body carries the sensors used in the IoT. These sensors are sensed by all significant information about the patient. So, sensitive information of the patient should not be leaked to the external world. The sensor nodes in IoT-based healthcare applications collect the patient's sensitive data and forward it to a coordinator node. If the sensitive information is overheard by an attacker and the data are used for any illicit reason, then the patient may be seriously harmed. It is not enough to only protect secrecy [91]. Data should also be safe from outside modifications. In this case, if a patient's sensitive and essential data have been corrupted, this changed data will be transmitted to the coordinator. For life-critical patients, this lack of honesty results in serious harm. Data loss can also occur in poor communication environments. In terms of

performance and security, the implementation of emerging technology poses many challenges, and thus, applications for the IoT must be secured. It can have deadly consequences to reveal any part of an IoT healthcare system to a hacker, whether a terrorist, disgruntled individual, blackmailer, or any other malicious actor. Many researchers are fully working on the issue of protecting IoT systems, but since no system can be 100 percent safe, it is important to identify and measure appropriate risk by ethicists and medical, legal, security, and financial professionals.

Risk of Patients Privacy Exposure

Health information (HI) is a broad term that includes both safe health information (PHI), which includes unique identifiers that can be uniquely connected to the patient, and not easily identifiable de-identified health information (DHI) [92]. It is necessary to clarify here that DHI is not necessarily anonymous data; in fact, data can vary from completely anonymous to fully identifiable, varying according to the degree to which identity is retained, masked, or eliminated, depending on the effort, capacity, time, and cost needed for full identification [93].

In the data, a minimum degree of identification is also required so that health researchers can aggregate datasets or perform efficiency or policy analysis for greater social benefits. HIPAA's Privacy Rule offers detailed guidance for alternative methods of de-identification [94] to establish this safety level of identifiability, thus minimizing privacy risks for patients and allowing secure data sharing practices. Therefore, data processed for de-identification using the above methods, i.e., DHI, are considered safer to share than PHI. Vendors and product manufacturers who have collaborated with healthcare service providers are also subject to HIPAA regulations as protected organizations (CEs) or business associates (BAs), as mentioned earlier. Non-partnered persons are not subject to HIPAA legislation and are deemed to be non-covered organizations (NCEs).

Data Encryption

Universal dataencryption could be executed at three communication phases: connection encoding, node encoding, and end-to-end encoding. The communication acquired from the earlier connection will be decoded into a readable form for any transitional node in associated encryption, and the readable text will thereafter be encoded into scrambled text by utilizing the undisclosed key of the following connection [68, 91]. Unlike liaison encryption, node encryption doesn't require plaintext communications in the system node. So, node encryption can deliver huge network data protection. When utilizing end-to-end encryption, the message is not decrypted until it is forwarded to the destination. Since communications are continually existing as scrambled text all through to protect eHealth public services, vital organization procedures execute a significant function in the protection method. Nevertheless, the communication frequency could be greatly altered by intricate

encryption systems or transmission protocols, and also fail to perform data transmission. They must use important medical services that are not accessible. Scientific and cautious steps are needed to solve the hard equilibrium between safety, protection, and system application consumption [68, 91]. Protection matters have been key impediments to eHealth systems that deliver unremarkable assistance to the aging and weak individuals owing to the inadequate funds obtainable and confidentiality apprehensions.

Data Eavesdropping and Data Confidentiality

It is a form of threat that brings security threats to the protection of the medical records of patients. This involves the sniffing of vital medical information conveyed by the IoT sensor/device resulting in privacy risks in communication. Assume that unsecured medical data were distributed by an IoT sensor/device to adjacent or upstream nodes. By using a sniffing software tool, an intruder will eavesdrop on the health information by sniffing it. To collect the health data of the patients, any unauthorized person can use a powerful transmitted signal like a sniffer. In general, the patient's medical records are maintained in compliance with legal confidentiality obligations and are given access only to licensed caregivers. It is necessary to prevent intercepted storage or spying data as it flows through wireless connections [90].

Identity Threats and Privacy of Stored Data

The following guidelines should be considered to protect the privacy of information storage. Only the least possible amount of information that is required should be retained. In the event of compulsory retention, only personal information is preserved, and the based on "need-to-know" knowledge is taken out. Pseudonymization and anonymization may be used to hide the real identity connected to the stored data. A database could allow access only to statistical data (sum, average, count, etc.) without revealing any particular record. The appropriate technique could be to ensure that the output (typically aggregate queries) is independent of the absence or presence of a specific record, adding noise called differential privacy [95].

Threats of Cyber-Attacks on Privacy

Attacks are actions taken using different techniques and methods to damage a device or interrupt regular operations by leveraging vulnerabilities. Attackers initiate assaults, for either personal satisfaction or compensation, to achieve goals. Cyber-attacks will inject false information into a system, which causes IoT applications to suffer critical harm. In smart healthcare applications, it is important to provide the patient with the required degree of defense from cyber threats. The resource constrained existence of many IoT devices present in a smart home environment

does not, however, allow standard security solutions to be implemented. Due to rising threats and government regulations, cyber protection systems that protect networks and computers from cyber-attacks are becoming widespread. At the same time, the vast volume of information collected by cyber security systems poses a significant threat to the privacy of those who are secured by them.

Location Privacy

Location privacy is concerned with threats to the privacy of locations and eavesdropping on the location of a device. By routing to a randomly chosen intermediate node (RRIN), location privacy in WSNs, precisely hiding the location of the message sender, can be accomplished [96]. The Location Privacy Routing (LPR) protocol, which uniformly distributes the directions of incoming and outgoing traffic at sensor nodes, will prevent packet dropping and tracing [97]. Phantom single-path routing ensures that packets follow different paths to the Base Station (BS) in such a way that each packet generated by a source follows a different random path to the BS [98].

6.5 Framework for Secure Transmission of Healthcare Information on IoT-Based Platform

The IoT provides computing tools as extremely flexible as web services. With the rapid growth of IoT and cloud computing technology, a growing number of individuals, organizations, and businesses prefer IoT and cloud platforms for storing and manipulating their data. Cloud computing has major benefits including cloud storage, connectivity, data sharing, and hardware and software cost savings. Many security challenges attributed to the IoT environment, however, have not yet been addressed, especially in traditional computer environments [66, 67]. Moreover, protection and privacy concerns have been observed to seriously limit the practical implementations of IoT technologies [66]. To tackle these major problems, it is important to propose and develop new algorithms and methods to secure the IoT platform and infrastructure.

The safety and confidentiality of records relating to patients are twofold essential notions. When we refer to record safety, this signifies that records are securely stowed and transmitted to ensure their absoluteness, genuineness, and legitimacy. Record confidentiality signifies that records can solitary be obtained by individuals who are authorized to sight and utilized it [68, 69]. More rational security measures may be established with different objectives and specifications in mind. The extensive utilization of IoT gadgets offers an improved assurance of an individual's health [70], but it also places a great deal of demand on record safety and concealment.

Consequently, efficacious IoT advancement needs to accept safety and confidentiality as an essential concentration. Although most healthcare establishments don't devote sufficient funds to shield safety and confidentiality [68, 99], there isn't any hesitation that safety and confidentiality perform a significant function in IoT. IoT gadgets create a growing amount of ever more complex real-time records, which is extremely delicate. On one side, the failure of health organization or system security may have catastrophic consequences. On the other hand, privacy information for the patient is accessible at all levels of record processing, record transfer, cloud storage, and record republication.

In this section, this chapter suggested an enhanced novel method built on an amalgamation of security procedures in each layer to hide the undisclosed message into a cover object to deliver satisfactory fortification for the concealed message transmission utilizing a standard IoT transmission channel. This approach will positively achieve the targeted standard of certain critical characteristics such as information confidentiality, efficiency and sturdiness, proof of the outstanding performance, and efficient application of this method. The primary goal of protection can be reached in the field of data transmission through the IoT-based system.

The secure transmission of medical information on the IoT environment was displayed in Fig. 6.2. The framework comprises certification manager, information manager, personal medical information encryption, security access control, and medical data confidentiality for the smart healthcare system. The framework consists of a service provider who updates healthcare data locally and transmits it through certification manager smart healthcare (medical institution). The authentication institution is called a healthcare certification manager, and they are in charge of key creation, management, and distribution including the role of intermediate for information and endorsement. The information manager in smart healthcare responsible for verification establishment that encrypts provides personal and medical information for storing data in the cloud database. The main function of the layer is for the independence of data provided by medical institutions to separate the function of smart healthcare information manager block. The layer also performing the encryption and authentication of the data, which in turn provides information decryption.

6.6 The Results and Discussion

The functions of the layers in the proposed framework are discussed in this section: the framework will be able to secure the medical information on the IoT-based platform.

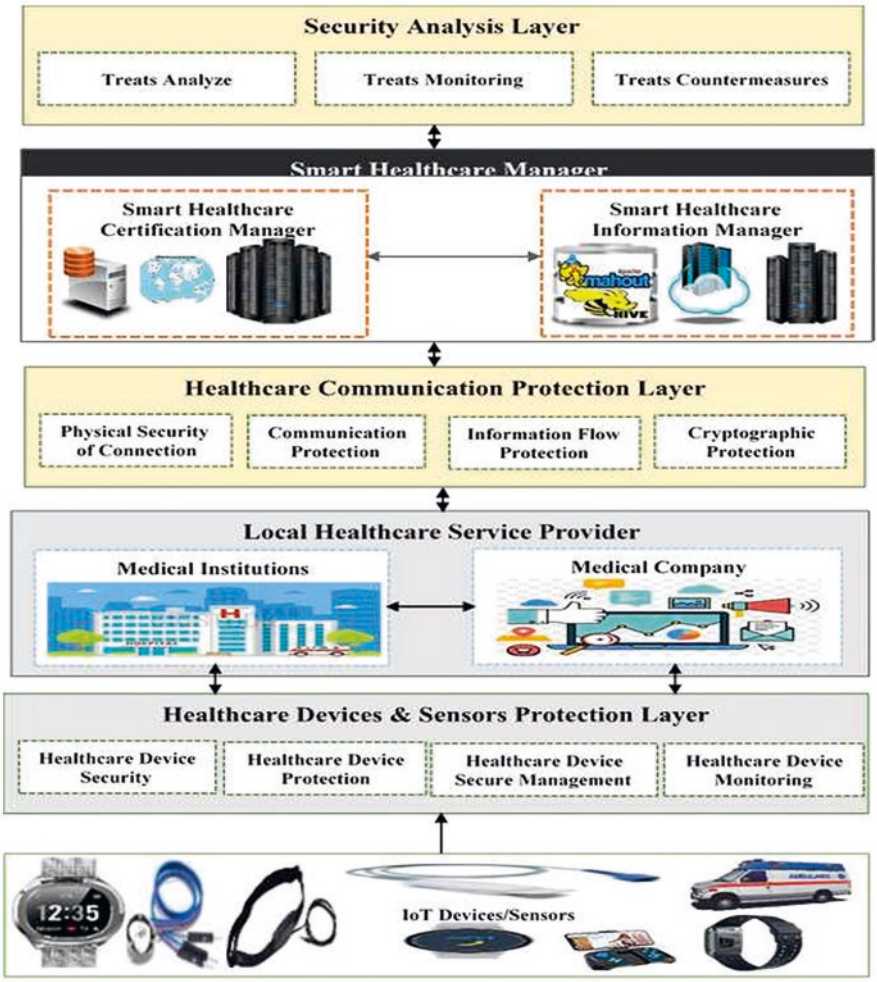

Fig. 6.2 The framework of a secure medical information on IoT-based environment

6.6.1 Healthcare Device Protection Layer

The protection layer employed anti-theft and intrusion mechanisms to prevent alteration and removal of the terminal. The confidentiality, integrity, and availability are maintained in this layer, by seeing to the functionality of the smart devices. This security was able to prevent the uncontrollable alteration of an attached device from the IoT platform by providing physical protection function using the provided techniques. The device monitoring scrutinized the process and the status of the terminal, error detection using equivalent data, and established countermeasures. Integrity review, malicious usage pattern identification, service denial operations are tracked

and scrutinized to trace its security routine directory. The terminal integrity was protected by the device protection by ensuring that the terminal is working under the settings required to perform within specified utilities. For the integrity of the terminal functions, the boot phase of the terminal and the execution of the terminal operation is tested.

6.6.2 Healthcare Communication Protection Layer

Information exchange between terminals of the IoT-based system was supported by the communication protection layer. This was made possible with the communication feature that provides interoperability between different devices. As threats to such information sharing, the degree of security needed for the communication role of IoT services needs to be prepared. Link physical protection covers the layers of physical links (e.g., cables) in the network. Security functions like encryption are given by the communication security block between terminals. Most IoT apps analyze features, including authentication and encryption, and use standardization protocols that have been reviewed. To secure the reliability of the communication, encryption technology with the integrity and confidentiality of communication records is used on the communication organizations. The destination device and network are transferred by the information flow protection block on the message types and content permitted using network integration and borderline fortification tools. All components of the network are being managed by the network management block monitor updates and maintain entirely communication protection policies, including network breakdown, password protected communication settings, and configuration of the firewall.

6.6.3 Security Analysis Layer

The layer analyzed data collected from the overall status data from terminals in addition to the network traffic to identify responses to security breaks or coercions to the system. This was done to identify in real-time some attack circumstances to device trends and set up countermeasures against such situations. This can be done using the intrusion activity pattern with an access control strategy from the gathered protection status data from the IoT-based environment. The analysis feature looks for events or patterns that may cause a particular device to have security vulnerabilities or threats. Malicious conduct analysis and rule-based analysis are performed at this level. The malicious behavior analysis discovers abnormal activities by scrutinizing usage trends in the system after studying normal activities. The events that do not occur in a normal system were analyzed using rule-based and, according to the established rules, define security threats. In the case of a security incident, it analyzes intrusion actions and suggests countermeasures. Before a security attack

happens, this feature prepares for security incidents by security policies. The identification and recovery of threats work to detect an existing safety incident and to restore the damage to normal status. In the event of an attack or security incident, the security forensics feature examines basic vulnerabilities and abuse cases.

The communication layer with numerous radar gadgets and items which can be linked over a radio receiver link supports information exchange between terminals. This radio receiver link could be separate from WiFi, ultra-wideband, RFID, ZigBee, and Bluetooth. The IoT gateway tolerates cyberspace and numerous networks to connect. The upper level is about big data analytics, where vast volumes of data obtained from radars are processed in the cloud and accessible by big data analytics apps. These frameworks provide API monitoring and a dashboard to aid in managing engine communication.

6.7 Conclusion

The integration of computer and biomedical technologies in medical systems has supported healthcare events, for instance, real-time disease analysis, remote monitoring of patients, and real-time drug prescriptions, among others. The methods have significantly helped to store both patients' personal information and their symptoms on the cloud, which can help during contagious diseases. This aids the quality of services provided by the physicians, thereby improving patients' satisfaction. But there are still security and privacy challenges face by IoT-based healthcare system, and many users are not ready to use the IoT-based platform. Therefore, this chapter presents a summary of the IoT-based architecture by discussing the privacy and security issues in IoT healthcare applications. This chapter also proposed a framework to secure healthcare information on the IoT-based platform. This chapter also demonstrates the architecture of the extensive healthcare system based on IoT, the technological problems, and some standard implementations relevant to comprehensive healthcare. Data safety, privacy, and confidentiality were looked into IoT-based security and privacy in healthcare systems. The proposed architecture has four layers; this was proposed in other to fully secure the IoT environments at all levels of the healthcare system. To provide verification, entry control, network, and device protection, integrity, and confidentiality, the framework model uses the features of the IoT environment. To eliminate all security threats in advance may be very difficult due to the use of diverse devices and technological rudiments of sensors used in healthcare systems, the security specifications suggested in this study are intended to contribute to the creation of secure IoT environments. This chapter concluded that the current framework will go a long way to help in protecting the sensors and devices use in the IoT-based environment at a different level of the system. The full implementation of the proposed scheme will be tested in future work.

References

1. Firouzi, F., Rahmani, A. M., Mankodiya, K., Badaroglu, M., Merrett, G. V., Wong, P., & Farahani, B. (2018). Internet-of-things and big data for smarter healthcare: From device to architecture, applications, and analytics.
2. Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues on the internet of things. In *The internet of things* (pp. 389–395). Springer.
3. Yang, P., Wu, W., Moniri, M., & Chibelushi, C. C. (2012). Efficient object localization using sparsely distributed passive RFID tags. *IEEE Transactions on Industrial Electronics, 60*(12), 5914–5924.
4. Adeniyi, E. A., Ogundokun, R. O., & Awotunde, J. B. (2021). IoMT-based wearable body sensors network healthcare monitoring system. In *IoT in healthcare and ambient assisted living* (pp. 103–121). Springer.
5. Riggins, F. J., & Wamba, S. F. (2015, January). Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In 2015 48th Hawaii international conference on system sciences (pp. 1531–1540). IEEE.
6. Yaqoob, I., Hashem, I. A. T., Gani, A., Mokhtar, S., Ahmed, E., Anuar, N. B., & Vasilakos, A. V. (2016). Big data: From beginning to the future. *International Journal of Information Management, 36*(6), 1231–1247.
7. Pramanik, P. K. D., Upadhyaya, B. K., Pal, S., & Pal, T. (2019). Internet of things, smart sensors, and pervasive systems: Enabling connected and pervasive healthcare. In *Healthcare data analytics and management* (pp. 1–58). Academic.
8. Darwish, A., Ismail Sayed, G., & Ella Hassanien, A. (2019). The impact of implantable sensors in biomedical technology on the future of healthcare systems. Intelligent pervasive computing systems for smarter healthcare (pp. 67–89).
9. Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IOMT): Applications, benefits, and future challenges in the healthcare domain. *The Journal of Communication, 12*(4), 240–247.
10. Manogaran, G., Chilamkurti, N., & Hsu, C. H. (2018). Emerging trends, issues, and challenges on the internet of medical things and wireless networks. *Personal and Ubiquitous Computing, 22*(5–6), 879–882.
11. Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: A survey of emerging technologies. *IEEE Communications Surveys and Tutorials, 22*(2), 1121–1167.
12. Akhtar, P., Khan, Z., Rao-Nicholson, R., & Zhang, M. (2019). Building relationship innovation in global collaborative partnerships: Big data analytics and traditional organizational powers. *R&D Management, 49*(1), 7–20.
13. Chan, M. M., Plata, R. B., Medina, J. A., Alario-Hoyos, C., Rizzardini, R. H., & de la Roca, M. (2018). Analysis of behavioral intention to use cloudbased tools in a MOOC: A technology acceptance model approach. *Journal of Universal Computer Science, 24*(8), 1072–1089.
14. Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues in fog computing: A survey. *Future Generation Computer Systems, 88*, 16–27.
15. Karati, A., Islam, S. H., Biswas, G. P., Bhuiyan, M. Z. A., Vijayakumar, P., & Karuppiah, M. (2017). Provably secure identity-based signcryption scheme for the crowdsourced industrial internet of things environments. *IEEE Internet of Things Journal, 5*(4), 2904–2914.
16. Solomon, M., & Elias, E. P. (2018). Privacy protection for wireless medical sensor data. *International Journal of Scientific Research in Science and Technology, 4*, 1439–1440.
17. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal, 5*(4), 2483–2495.
18. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificates authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications, 106*, 117–123.

19. Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2017). Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. *IEEE Internet of Things Journal, 5*(4), 2884–2895.
20. Luo, E., Liu, Q., & Wang, G. (2016). Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks. *IEEE Communications Letters, 20*(9), 1772–1775.
21. ur Rehman, M. H., Yaqoob, I., Salah, K., Imran, M., Jayaraman, P. P., & Perera, C. (2019). The role of big data analytics in industrial internet of things. *Future Generation Computer Systems, 99*, 247–259.
22. Pace, P., Aloi, G., Gravina, R., Caliciuri, G., Fortino, G., & Liotta, A. (2018). An edge-based architecture to support efficient applications for healthcare industry 4.0. *IEEE Transactions on Industrial Informatics, 15*(1), 481–489.
23. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges. *IEEE Wireless Communications, 23*(5), 10–16.
24. Pace, P., Aloi, G., Caliciuri, G., Gravina, R., Savaglio, C., Fortino, G., … & Mortara, M. (2019, April). Inter-health: An interoperable IoT solution for active and assisted living healthcare services. In 2019 IEEE 5th world forum on internet of things (WF-IoT) (pp. 81–86). IEEE.
25. Veltink, P. H., Bussmann, H. J., De Vries, W., Martens, W. J., & Van Lummel, R. C. (1996). Detection of static and dynamic activities using uniaxial accelerometers. *IEEE Transactions on Rehabilitation Engineering, 4*(4), 375–385.
26. Lyons, G. M., Culhane, K. M., Hilton, D., Grace, P. A., & Lyons, D. (2005). A description of an accelerometer-based mobility monitoring technique. *Medical Engineering & Physics, 27*(6), 497–504.
27. Luštrek, M., & Kaluža, B. (2009). Fall detection and activity recognition with machine learning. *Informatica, 33*(2).
28. Pappas, I. P., Popovic, M. R., Keller, T., Dietz, V., & Morari, M. (2001). A reliable gait phase-detection system. *IEEE Transactions on Neural Systems and Rehabilitation Engineering, 9*(2), 113–125.
29. Paganelli, F., & Giuli, D. (2007, May). An ontology-based context model for home health monitoring and alerting in chronic patient care networks. In 21st international conference on advanced information networking and applications workshops (AINAW'07) (Vol. 2, pp. 838–845). IEEE.
30. Salarian, A., Russmann, H., Wider, C., Burkhard, P. R., Vingerhoets, F. J., & Aminian, K. (2007). Quantification of tremor and bradykinesia in Parkinson's disease using a novel ambulatory monitoring system. *IEEE Transactions on Biomedical Engineering, 54*(2), 313–322.
31. Moncada-Torres, A., Leuenberger, K., Gonzenbach, R., Luft, A., & Gassert, R. (2014). Activity classification is based on inertial and barometric pressure sensors at different anatomical locations. *Physiological Measurement, 35*(7), 1245.
32. Bianchi, F., Redmond, S. J., Narayanan, M. R., Cerutti, S., & Lovell, N. H. (2010). Barometric pressure and triaxial accelerometry-based fall event detection. *IEEE Transactions on Neural Systems and Rehabilitation Engineering, 18*(6), 619–627.
33. Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of the internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems. *Journal of Ambient Intelligence and Humanized Computing, 10*(10), 4151–4166.
34. Mukherjee, P., & Mukherjee, A. (2019). Advanced processing techniques and secure architecture for sensor networks in ubiquitous healthcare systems. In *Sensors for health monitoring* (pp. 3–29). Academic.
35. Ismail, W. N., Hassan, M. M., Alsalamah, H. A., & Fortino, G. (2020). CNN-based health model for regular health factors analysis in internet-of-medical things environment. *IEEE Access, 8*, 52541–52549.

36. Wang, N., Deng, Z., Wen, L. M., Ding, Y., & He, G. (2019). Understanding the use of smartphone apps for health information among pregnant Chinese women: Mixed methods study. *JMIR mHealth and uHealth, 7*(6), e12631.
37. Le Kernec, J., Fioranelli, F., Ding, C., Zhao, H., Sun, L., Hong, H., … Romain, O. (2019). Radar signal processing for sensing in assisted living: The challenges associated with the real-time implementation of emerging algorithms. *IEEE Signal Processing Magazine, 36*(4), 29–41.
38. Farahani, B., Firouzi, F., & Chakrabarty, K. (2020). Healthcare IoT. In *Intelligent internet of things* (pp. 515–545). Springer.
39. Padmavathi, S. (2020). A fog-based approach for real-time analytics of IoT-enabled healthcare. In *The internet of things use cases for the healthcare industry* (pp. 43–66). Springer.
40. Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., & Schreier, G. (2010, April). The internet of things for ambient assisted living. In 2010 seventh international conference on information technology: new generations (pp. 804–809). IEEE.
41. Brownsell, S., & Hawley, M. (2004). Fall detectors: Do they work or reduce the fear of falling? *Housing, Care, and Support, 7*(1), 18.
42. Wagner, F., Basran, J., & Dal Bello-Haas, V. (2012). A review of monitoring technology for use with older adults. *Journal of Geriatric Physical Therapy, 35*(1), 28–34.
43. Nguyen, H. H., Mirza, F., Naeem, M. A., & Nguyen, M. (2017, April). A review of 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) (pp. 257–262). IEEE.
44. Kalid, N., Zaidan, A. A., Zaidan, B. B., Salman, O. H., Hashim, M., & Muzammil, H. (2018). Based on real-time remote health monitoring systems: A review on patients' prioritization and related "big data" using body sensors information and communication technology. *Journal of Medical Systems, 42*(2), 30.
45. Ayo, F. E., Ogundokun, R. O., Awotunde, J. B., Adebiyi, M. O., & Adeniyi, A. E. (2020, July). Severe acne skin disease: A fuzzy-based method for diagnosis. Lecture notes in computer science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020, 12254 LNCS (pp. 320–334).
46. Azimi, I., Rahmani, A. M., Liljeberg, P., & Tenhunen, H. (2017). Internet of things for remote elderly monitoring: A study from a user-centered perspective. *Journal of Ambient Intelligence and Humanized Computing, 8*(2), 273–289.
47. Fortino, G., Gravina, R., & Galzarano, S. (2018). *Wearable computing: From modeling to implementation of wearable systems based on body sensor networks*. John Wiley & Sons.
48. Zheng, M., Liu, P. X., Gravina, R., & Fortino, G. (2018). An emerging wearable world: New gadgetry produces a rising tide of changes and challenges. *IEEE Systems, Man, and Cybernetics Magazine, 4*(4), 6–14.
49. Fortino, G., Giannantonio, R., Gravina, R., Kuryloski, P., & Jafari, R. (2012). Enabling effective programming and flexible management of efficient body sensor network applications. *IEEE Transactions on Human Machine Systems, 43*(1), 115–133.
50. Fortino, G., Guerrieri, A., Bellifemine, F., & Giannantonio, R. (2009, October). Platform-independent development of collaborative wireless body sensor network applications: SPINE2. In 2009 IEEE international conference on systems, man and cybernetics (pp. 3144–3150). IEEE.
51. Lee, S. Y., Chou, C. L., Hsu, S. P., Shih, C. C., Yeh, C. C., Hung, C. J., … Liao, C. C. (2016). Outcomes after stroke in patients with previous pressure ulcer: A Nationwide matched retrospective cohort study. *Journal of Stroke and Cerebrovascular Diseases, 25*(1), 220–227.
52. Jaul, E., & Menzel, J. (2014). Pressure ulcers in the elderly, as a public health problem. *Journal of General Practice, 2*, 5.
53. Pal, D., Triyason, T., & Funikul, S. (2017, December). Smart homes and quality of life for the elderly: A systematic review. In 2017 IEEE international symposium on multimedia (ISM) (pp. 413–419). IEEE.
54. Tun, S. Y. Y., Madanian, S., & Mirza, F. (2020). Internet of things (IoT) applications for elderly care: A reflective review. *Aging Clinical and Experimental Research*, 1–13.

55. Shany, T., Redmond, S. J., Marschollek, M., & Lovell, N. H. (2012). Assessing fall risk using wearable sensors: A practical discussion. *Zeitschrift für Gerontologie und Geriatrie, 45*(8), 694–706.
56. Sharma, C. A., Kumar, A. K. S. V., Prasad, A., Begum, R., Sharvani, G. S., & Manjunath, A. E. (2018, January). Multifaceted bio-medical applications of exoskeleton: A review. In 2018 2nd international conference on inventive systems and control (ICISC) (pp. 11–15). IEEE.
57. Oladele, T. O., Ogundokun, R. O., Awotunde, J. B., Adebiyi, M. O., & Adeniyi, J. K. (2020, July). Diagmal: A malaria coactive neuro-fuzzy expert system. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2020, 12254 LNCS (pp. 428–441).
58. Yein, N., & Pal, S. (2017, January). Technological assistance for falls among the aging population: A review. In *International conference on research into design* (pp. 409–419). Springer.
59. De Bruin, E. D., Hartmann, A., Uebelhart, D., Murer, K., & Zijlstra, W. (2008). Wearable systems for monitoring mobility-related activities in older people: A systematic review. *Clinical Rehabilitation, 22*(10–11), 878–895.
60. Amaraweera, S. P., & Halgamuge, M. N. (2019). Internet of things in the healthcare sector: Overview of security and privacy issues. In *Security, privacy, and trust in the IoT environment* (pp. 153–179). Springer.
61. Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2018). Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet of Things Journal, 6*(1), 410–420.
62. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous patient monitoring with a patient-centric agent: A block architecture. *IEEE Access, 6*, 32700–32726.
63. Vermesan, O., & Friess, P. (Eds.). (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). River Publishers.
64. Malan, D. J., Fulford-Jones, T., Welsh, M., & Moulton, S. (2004). Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In International workshop on wearable and implantable body sensor networks.
65. Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors, 12*(1), 55–91.
66. Abdulraheem, M., Awotunde J. B., Jimoh, R. G., & Oladipo, I. D. (2021). An efficient lightweight crypotographic Algorithm for IoT security. *Communication in Computer and Information Science, 1350*, 444–456.
67. Mutlag, A. A., Ghani, M. K. A., Arunkumar, N. A., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems, 90*, 62–78.
68. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: A review. *Security and Communication Networks, 2018*.
69. Tang, J., Liu, A., Zhao, M., & Wang, T. (2018). An aggregate signature based trust routing for data gathering in sensor networks. *Security and Communication Networks, 2018*.
70. Sun, W., Cai, Z., Liu, F., Fang, S., & Wang, G. (2017, October). A survey of data mining technology on electronic medical records. In 2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom) (pp. 1–6). IEEE.
71. Thomas, C. (2020). Introductory chapter: Computer security threats. In *Computer security threats*. IntechOpen.
72. Jones, J. C. (2016). Nurses rank as most honest, ethical profession for 14th straight year.
73. Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures, and security issues: A comprehensive survey. *Sensors, 18*(9), 2796.
74. Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications, 78*(23), 32633–32657.

75. Tsai, C. W., Lai, C. F., Chao, H. C., & Vasilakos, A. V. (2015). Big data analytics: A survey. *Journal of Big Data, 2*(1), 1–32.
76. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. *IEEE Access, 5*, 5247–5261.
77. Fortino, G., Guerrieri, A., Bellifemine, F. L., & Giannantonio, R. (2009, July). SPINE2: Developing BSN applications on heterogeneous sensor nodes. In 2009 IEEE international symposium on industrial embedded systems (pp. 128–131). IEEE.
78. Iyengar, S., Bonda, F. T., Gravina, R., Guerrieri, A., Fortino, G., & Sangiovanni-Vincentelli, A. (2008, March). A framework for creating healthcare monitoring applications using wireless body sensor networks. In proceedings of the ICST 3rd international conference on body area networks (pp. 1–2).
79. Fortino, G., Galzarano, S., Gravina, R., & Li, W. (2015). A framework for collaborative computing and multi-sensor data fusion in body sensor networks. *Information Fusion, 22*, 50–70.
80. Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., & Savaglio, C. (2016, April). A mobile multi-technology gateway to enable IoT interoperability. In 2016 IEEE first international conference on internet-of things design and implementation (IoTDI) (pp. 259–264). IEEE.
81. Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., & Kanhere, S. S. (2020). Blockchain technologies for IoT. In *Advanced applications of blockchain technology* (pp. 55–89). Springer.
82. Suresh, A., Nandagopal, M., Raj, P., Neeba, E. A., & Lin, J. W. (2020). *Industrial IoT application architectures and use cases*. CRC Press.
83. Glaroudis, D., Iossifides, A., & Chatzimisios, P. (2020). The survey, comparison, and research challenges of IoT application protocols for smart farming. *Computer Networks, 168*, 107037.
84. Nie, X., & Zhong, X. (2013, March). Security in the internet of things based on RFID: Issues and current countermeasures. In *Proceedings of the 2nd international conference on computer science and electronics engineering*. Atlantis Press.
85. Fathy, M., Samouti, S. A., Samouti, A., & Senior, I. T. (2016). NFC threats and attacks: Applying a low cost algorithm for secure channel using Twofish. *Bulletin de la Société Royale des Sciences de Liège, 85*, 1475–1486.
86. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the internet of things. *Digital Communications and Networks, 4*(2), 118–137.
87. Bayat, M., Beheshti-Atashgah, M., Barari, M., & Aref, M. R. (2019). Cryptanalysis and improvement of a user authentication scheme for the internet of things using elliptic curve cryptography. *IJ Network Security, 21*(6), 897–911.
88. Puthal, D., Yang, L. T., Dustdar, S., Wen, Z., Jun, S., Moorsel, A. V., & Ranjan, R. (2020). A user-centric security solution for the internet of things and edge convergence. *ACM Transactions on Cyber-Physical Systems, 4*(3), 1–19.
89. Anand, S., & Sharma, A. (2020). Assessment of security threats on IoT based applications. *Materials Today: Proceedings*.
90. Ayo, F. E., Folorunso, S. O., Abayomi-Alli, A. A., Adekunle, A. O., & Awotunde, J. B. (2020). Network intrusion detection is based on deep learning model optimized with rule-based hybrid feature selection. *Information Security Journal: A Global Perspective, 29*, 1–17.
91. Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). A safe and secured iris template using steganography and cryptography. *Multimedia Tools and Applications, 79*(31–32), 23483–23506.
92. Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society, 34*(1), 49–57.
93. Nelson, G. S. (2015). Practical implications of sharing data: A primer on data privacy, anonymization, and de-identification. In SAS global forum proceedings (pp. 1–23).

94. Portability, I. (2012). Guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability act (HIPAA) privacy rule.
95. Hall, R., Rinaldo, A., & Wasserman, L. (2013). Differential privacy for functions and functional data. *Journal of Machine Learning Research, 14*(Feb), 703–727.
96. Gupta, S., Kumar, P., Singh, J. P., & Singh, M. P. (2016). Privacy preservation of source location using phantom nodes. In *Information technology: New generations* (pp. 247–256). Springer.
97. Yao, L., Kang, L., Shang, P., & Wu, G. (2013). Protecting the sink location privacy in wireless sensor networks. *Personal and Ubiquitous Computing, 17*(5), 883–893.
98. Manjula, R., & Datta, R. (2018). A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs. *Pervasive and Mobile Computing, 44*, 58–73.
99. Huang, M., Liu, A., Wang, T., & Huang, C. (2018). Green data gathering under delay differentiated services constraint for the internet of things. *Wireless Communications and Mobile Computing, 2018*.