Chapter 8

Healthcare monitoring through IoT: security challenges and privacy issues

S.O. Owoeye[1], A.S. Akinade[1], K.I. Adenuga[2] and F.O. Durodola[1]

Abstract

With a projected increase in world population to about 2.3 billion by the year 2050 and the corresponding challenges this increase would have on the provision of healthcare for the populace, there arises a need for a drastic improvement in the current state of the healthcare industry in order to overcome the challenges. A shift from the usual reactive approach to healthcare, in which health conditions would have deteriorated before treatment begins, to a more proactive methodology, which focuses on early diagnosis, identification and prevention of health conditions and wellness management is needed. This can be achieved by making health condition monitoring and well-being management a huge priority. Thus, considerations must be given to Internet of Things (IoT) technologies, as they can impact positively in designing, building and maintaining intelligent, interconnected and individually tailored healthcare services and products. With the aid of IoT technologies, individual physical conditions can be monitored continuously and remotely and actions are taken as necessary. Also, a proper record can be kept for individual health conditions and their progress levels monitored, thus, enabling healthcare providers to better evaluate and detect early symptoms of health problems. Although with the adoption of the IoT in healthcare, a lot of benefits are obtainable, there are still some concerns, including security, standards, scalability and privacy. These concerns seem to overwhelm the seemingly broad opportunities available in IoT and must be tackled to facilitate the application of IoT. This chapter aims to open up the techniques and advantages of IoT in personalized healthcare. It also opens up the challenges and possible solutions that can be adopted in tracking and monitoring health status.

Keywords: Diagnosis; Healthcare; Internet of Things; Security; Symptoms; Treatment; Privacy

[1]Department of Mechatronics Engineering, Federal University of Agriculture, Abeokuta, Nigeria
[2]Farnborough College of Technology, University Centre Farnborough, Farnborough, United Kingdom

8.1 Introduction

Over the past years, the usage of the Internet of Things (IoT) has continued to witness an exponentially increase in its application in the field of information and communication technology and is also tagged the future of the technical revolution. It is a popular belief that the total amount of devices currently connected over IoT (about 12 million devices) will witness an exponential increase in the nearest foreseeable future [1]. IoT is used to describe devices and equipment that are capable of communicating and interacting with the Internet through physical devices, sensors, microcontrollers and network connectivity to collect and exchange data. In a bid to ensure consistent real-time data collection, each device in the system is tagged with a unique identifier, which allows seamless communication between each machine, and the data collected from various devices in various locations around the globe are to be stored in cloud storage, thus making our systems more efficient and smarter. Smart objects, which are the fundamental foundation on which the process of refining the cyber-physical smart universal frameworks are implemented, were created by IoT. The IoT is targeted toward the interconnectivity of an unlimited amount of physical devices or equipment that would have various sensors and actuators embedded in them, being enabled by different access networks through the aid of technologies, including wireless sensor networks (WSN), radio-frequency identification (RFID), real-time and semantic web services [2]. It becomes obvious that the areas of application of IoT are limitless due to its ability to facilitate communication between different physical objects and allow an easy operation of devices over the Internet [3]. The role of sensors in detecting signals cannot be overlooked as their roles are found in numerous applications, including smart devices and systems, automotive systems, climate monitoring, industrial control, healthcare and so on.

The idea of the IoT took off recently and it is defined as the combination of devices that, by possessing network connectivity, can be monitored and controlled from a web platform and also provides real-time information for subsequent uses [4]. In another theory, the IoT is referred to as things, especially commonly used devices and equipment that are distinguishable, identifiable, addressable and controllable over the Internet by using either RFID, wireless LAN, wide area network or other methods [5]. Kevin Ashton first used the word IoT in the year 1998, when he observed that three models can be used to define the Internet, namely, the sensors-oriented semantics, Internet-oriented middleware and knowledge-oriented semantics. Although it is important to note that IoT is more versatile when working across these three models in its different application scenarios. The applications of IoT in the various facets of our lives include smart car parking systems, smart homes and cities, industrial automation, smart agriculture and healthcare processes. One major example of IoT application in healthcare is in real-time health status monitoring of patients [6]. In recent times, IoT has increased its usefulness in the health sector, through the use of sensors and microcontrollers in the collection and analysis of data and also transferring to the cloud for access by caregivers (doctors and nurses). When IoT features are integrated into equipment and devices used in

the healthcare sector, the quality and value of care delivered to patients are greatly improved for different categories of patients with varying health conditions. Also, there is no restriction on the number of patients that can be monitored per time as patients' data are computerized, thus helping both patients and caregivers capture and monitor the data anytime from any location. These days, the majority of sensors used in the health sector are relatively small in size, making them wearable and closely connected to the patient for the doctor to monitor the patient's current condition irrespective of the time or location of the patient. This enables real-time diagnosis and prescriptions to be administered as and when necessary [1].

In many developing countries, their current infrastructure for supporting healthcare is not up to the minimum standard. To ensure that the general populace has unrestricted access to healthcare, the various wearable sensors can be equipped with communication capabilities with portable devices like smartphones and tablets, etc., which enables communication with the cloud and then the people can be provided with access to these devices to have access to real-time healthcare [7].

With the advent of IoT, medical records of patients are being transformed into data for smart healthcare delivery, thus making healthcare more technologically driven. IoT is capable of supporting applications that could potentially save lives in the healthcare sector by carrying out activities, including patient data and records collection from bedside and wearable devices, and real-time diagnosis of patients' conditions (see Figure 8.1).

Through the aid of IoT, caregivers or doctors do not need to pay a physical visit to the patient but can carry out monitoring, diagnosis and tracking of medical assets remotely. With the utilization of sensors and network connectivity, sensual

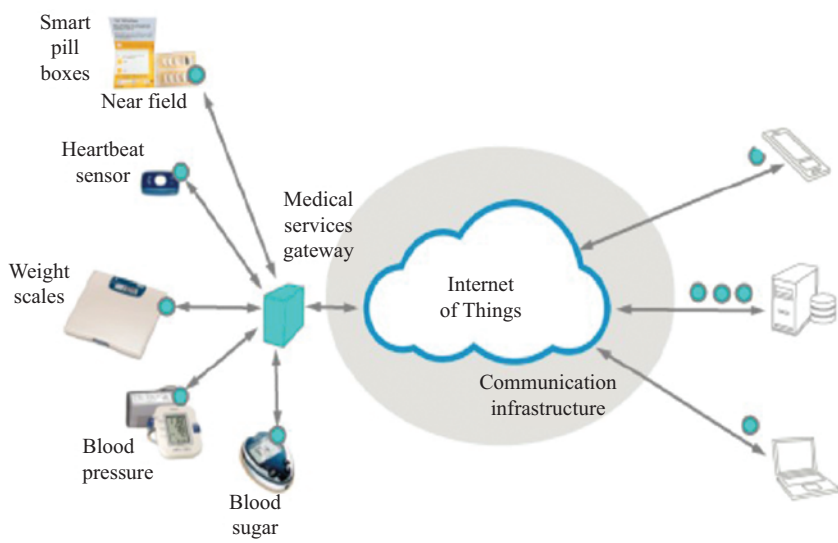

Figure 8.1 General IoT in healthcare [8]

information of patients can be retrieved from the necessary department, thus assisting the physician(s) to carry out more accurate diagnosis and treatment of patients, especially for those who are not physically available for on-the-spot operations.

In recent times, the number of people who are being diagnosed with chronic diseases is increasing daily, due to a lot of factors, including nutritional choices, physical inactivity, consumption of alcohol or toxic substances, environmental pollution, etc. According to the World Health Organization each year, an estimated 4.9 million people die as a result of the consumption of tobacco, 2.6 million deaths from overweight or obesity, 4.4 million from elevated cholesterol levels, 7.1 million deaths due to raised blood pressure (BP) and 1.9 million deaths due to lack of physical activity [9]. It is also forecasted that the number of deaths resulting from chronic diseases over the next 10 years will experience a drastic increase of 17%, resulting in about 64 million people deaths. Chronic diseases present a high level of variations in their symptoms as well as the way they evolve and techniques of treatment. Many of these diseases can lead to the death of the patient if not diagnosed and treated at their early stages. Some of the most chronic diseases that have possibilities of being treated include diabetes, BP and cardiac arrhythmia [9]. These chronic diseases often result in limitations to the physical mobility of patients that could also lead to socioeconomic and emotional related challenges [8]. In many cases, patients often find it hard to accept the reality of the long-term status of the disease, thus making adaptation difficult. This calls for constant monitoring by the doctor to constantly diagnose their health status and set treatment routines. In previous years, glucose and BP levels were measured by a physical examination in a specialized health facility, but with technological advancement, some sensors have been designed to do such measurements. Such sensors include a BP cuff, glucometer, heart rate monitor, etc.

One major concern in the evolution of humans is the health system with respect to technology development, the recent pandemic (COVID-19) shows a major example of how important standard healthcare is. In such situations, it is a better and safer approach to remotely monitor and diagnose patients, and healthcare systems equipped with the IoT could solve this challenge [10]. Remote patient monitoring enables the observational analysis of patients outside of the clinic environment and at their respective locations, thereby expanding access to healthcare services and reducing costs.

One common feature in the care delivered to critically ill patients is the repetitive measurement and diagnosis of patients body conditions, including heart rate and rhythm, respiratory rate, BP, blood oxygen saturation, blood sugar levels, etc. in instances where accurate and timely decision-making is required, electronic monitors play a crucial role in the collection and display of these data. Now, patients' data collection can be carried out using non-invasive sensors to record data that are routinely taken efficiently and detect conditions that could be life-threatening as quickly as possible [11].

The advent of IoT has allowed the number of people being cared for to increase and reduce overcrowding in healthcare facilities as the caregivers can attend to all patients placed under their care at any time and from any location without patients having to be physically present. For patients who require

continuous monitoring, IoT would enable them only to visit the physician physically after the proactive intervention. Therefore, many of the challenges the healthcare system is currently facing will be addressed as a load of patients in the facilities would reduce, and also travel time of physicians will be reduced and also create more time to be devoted to the patients with critical needs.

It is important to also mention that current monitoring systems allow patients to be placed under continuous monitoring of vital signs, but this system allows sensors to be placed in such a way that restricts patients' mobility by being attached to bedside monitors. In this case, there might be a wireless connection between the sensors and the monitors [12], but it requires the patient to be within a specified distance from the monitor such that outside that range, data collection becomes impossible. Nowadays, an increase in the dominance of chronic diseases poses a major challenge on individuals and society at large. These diseases could require continuous and constant treatment in the hospital to keep important parameters under control. In a bid to improve the quality of life of such patients, employing automatic devices to monitor biological parameters in real-time takes it a step further. Thus, creating an integration of mobile communications into these wearable sensors has set the ball rolling for the migration of healthcare services from being clinic-centric to one that is more patient-centric [13].

During the recent decade, the demographic changes in developed countries resulting in a more elderly population and the increasing prevalence of chronic diseases have contributed to the need for constant monitoring of the state of patients' health. According to the World Health Organization [14], chronic diseases such as coronary heart disease, cancer, chronic obstructive pulmonary disease and diabetes mellitus type 2 constitute the leading cause of mortality in the world, representing about 60% of all deaths. Chronic diseases are primarily attributable to heart failure, currently the main cause of death in most Western countries. The 2016 report of the American Heart Association on the Heart Disease and Stroke Statistics showed that 15.5 million people in the USA suffer from cardiovascular disease, this prevalence increasing with age for both women and men [15]. Chronic diseases also have a negative impact on the quality of people's life. Patients suffering from these pathologies must, often, carry out a monitoring of physiological parameters such as heart rate and BP as well as take control of the main risk factors that can aggravate their state of health. In less dangerous cases, it is convenient to monitor patients outside the hospital. On the one hand, such patients can face their illness in a family context that helps to speed up their recovery time. On the other, this strategy implies a considerable saving of resources, allowing social health facilities and personnel to be assigned to patients with more severe diseases.

8.2 IoT applications in personalized healthcare

8.2.1 In-clinic care

This application involves utilizing an IoT-controlled sensor to continuously monitor the patient, for whom close attention is a necessity due to their physiological

conditions. The condition of the patient is monitored with the aid of these sensors that use gateways to collect the needed physiological data and then stored in cloud storage for unrestricted access by caregivers and doctors who might require the data for further diagnosis as shown in Figure 8.2, thereby reducing the cost of healthcare for the patient and improving quality of care provided [16].

8.2.2 Remote monitoring

Generally, IoT applied to remote health monitoring systems operates by keeping a real-time track of crucial signs displayed by patients and providing a quick and proactive response in the advent of any problem with a patient's health. This device, when connected to the patient as shown in Figure 8.3, important information about patients' vital signs are transmitted from the patient's location to the hospital via a transmitter that establishes a connection over a telecom network [16].

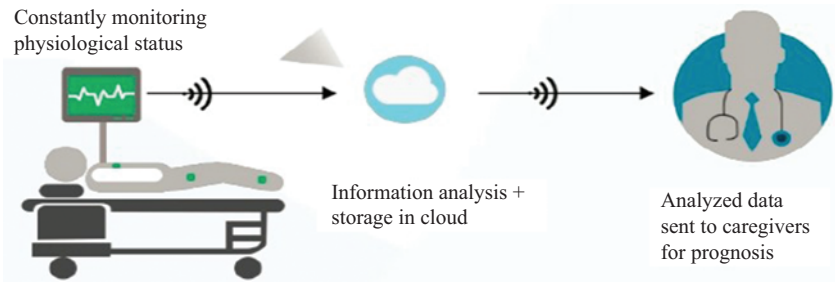

Figure 8.2 Clinical care system that constantly monitors the physiological status [17]

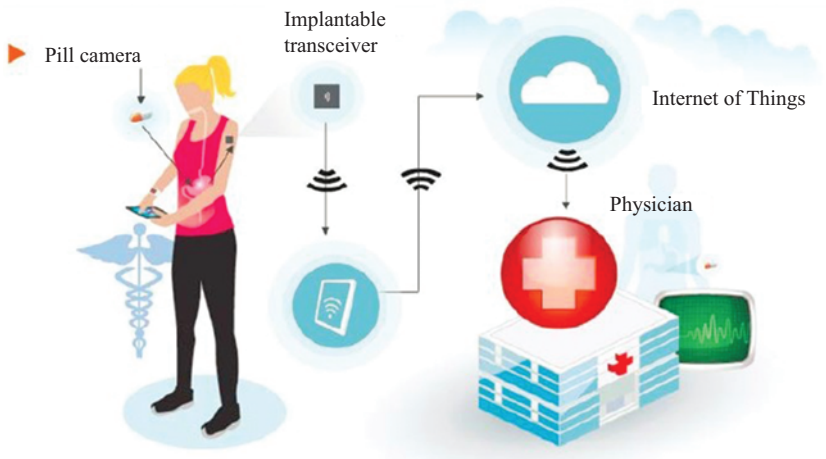

Figure 8.3 Remote health monitoring system [16]

In the hospital, there is a remote monitoring system that receives the data that has been transmitted and sends it securely to the caregivers.

8.2.3 Blood pressure monitoring

One important piece of physiological data that could be received from the human body is the BP and the most commonly used monitors are quite safe and easy to use [17]. With technological advancement in healthcare, the simple and electronic BP monitor is connected with an IoT sensor to enable real-time data collection and transmission of BP levels to the necessary quarters.

8.2.4 Rehabilitation system

A rehabilitation system is capable of restoring the lost functional abilities of people who are experiencing some form of disabilities, thereby improving the quality of their lives. It becomes very essential in mitigating challenges that are associated with the elderly ones, especially in cases of shortage of health personnel [10,17]. A convenient interaction and allocation of medical resources in respect to patient necessities can be done by an ontology-based automating designing method connected with an IoT-based smart rehabilitation system [18].

8.2.5 Oxygen saturation monitoring

To carry out continuous monitoring of a patient's blood oxygen saturation, in a non-invasive manner, a pulse-oximeter is used [17]. With the advancement in the field of communication technology, a lot of sensors used in the medical field are beginning to have low-power consumption and low-power loss, thereby making them very dominants. Pulse oximeters are employed for continuous monitoring in the medical field to keep track of the blood oxygen level and heart rate of patients. An IoT sensor, being attached to the body of the patient, will help to keep continuous track of these data in real-time [19].

8.2.6 Wheelchair management

When people suffer from a physical illness and find it difficult or unable to walk, the wheelchair becomes a saving grace. A sensor that senses humans could be connected over the Internet that detects when the human is falling off the wheelchair and can be monitored in real-time from the hospital. An acceleration sensor could be attached to the wheelchair to detect the falling of the wheelchair [20].

8.2.7 Healthcare solutions using smartphones

Healthcare professionals obtain numerous benefits from healthcare apps (Table 8.1) that provide on-the-go access to health records of patients, information about location and time of events or emergencies of patients, means of communication between doctors and patients and efficient and timely decision-making [21]. By using smartphone apps, in conjunction with sensors, the location and access to healthcare services have improved, thereby resulting in better results on patients' health conditions.

Table 8.1 General healthcare apps for smartphones [17]

Sl. No.	Healthcare app	Description
1	Calorie counter	Keeping track of the food that has been consumed and calculates the fat, weight as well as cholesterol present in the body
2	Heart rate monitor	It continuously monitors the heartbeat and collects relevant real-time information
3	Blood pressure monitor	It collects the blood pressure level of the patient, analyzes and records the data
4	Body temperature	Keeping track of the body temperature and alerting when the body temperature increased beyond set limits
5	Pedometer	It is used in recording the number of steps that have been walked and gives information about how many calories have been burned per unit of time
6	Water your body	The app is used to serve as a reminder to drink water every hour and also in tracking the human body water drinking habits
7	OnTrack Diabetes	It is used in the monitoring of the blood glucose level and administering proper medication in treating diabetes
8	Skin vision	It keeps on tracking the condition of the skin, thereby enabling us to identify early any skin disorder that occurs
9	Eye Care	It monitors the eyes vision and then is analyzed and tested
10	Asthma trackers and log	It monitors real-time information of the patients' asthma
11	CardioMobile	It monitors cardiac rehabilitation that is done remotely on a real-time basis and collects the data
12	Pill reminder	It serves as a reminder for the patient on the use of their medication at the appropriate time
13	Fall detector	This continuously monitors the rate of human activity and alerts in case there are issues

8.3 Challenges of IoT in personalized healthcare

The IoT exceeds a conventional computer-based model but is more of an interconnected model of distributed devices. Modern applications in IoT create an avenue for IoT services to integrate and use data from various devices. IoT builds a complex system with basic features for detecting the status of the environment, recording physiological data of humans, operational data of machines, detecting and differentiating between humans, animals, events and other nonliving objects in the environment, with additional capabilities of communicating with other devices [22]. In addition, the system can convert these data into instructions that drive automation and provide some form of feedback to the system via the specified communication networks to create actuation and control for other processes. Clearly, in this complex, interconnected and heterogeneous model, there is bound to be a lot of challenges associated with IoT. These challenges include, but are not limited to, the following:

1. Security and privacy: There could be a lot of situations that the devices connected in the IoT, such as smartphones, sensors, etc., could be exposed to risk

from hackers or hacking [1]. Thus, encryption must be carried out in instances when data are required to be exchanged between devices.

2. Integration: Another challenge faced by IoT in the healthcare sector is the integration of diverse protocols and different devices within the framework of the network. The numerous devices all collect data and transmit over different communication protocols in the same network, thereby making it complicated [23].
3. Technology adoption: In many cases, it is not enough to introduce a new technology that could help both patients and doctors, but more importantly its easy acceptance, adoption and usage are vital, which would help monetization easy in the healthcare system [24].

8.4 Security of IoT in personalized healthcare

With the increasing number of devices connected over communication networks in IoT, there is an increasing risk in their security as new challenges are posed. When a device is capable of Internet connection, there is a transfer of security risks faced by modern computing devices. Thus, there are basic security requirements that should be considered. These requirements include authorization, authentication, confidentiality, trust and data security. In other words, there should be a secure connection between devices over their dedicated networks, which has strict control and restricted access to only authorized users. The data that are of concern have to possess some level of security in collection, analysis, storage and transmission. Notwithstanding the risks associated with human–machine communications, there are also security risks in machine–machine communications. For instance, when there needs to be a form of access from human users to the devices, some security protocol has to be put in place. These protocols ensure that these devices are giving access to authorized personnel only and are not revealing private and confidential information to unauthorized users or for miscellaneous use.

8.4.1 The inherited security challenges in the IoT

In other terms, IoT can be referred to as Internet 2.0 or the future Internet. IoT is not a standalone form of communication or networks running differently or simultaneously with the Internet. Rather, it is an expansion of the Internet. This means that IoT inherits some of the security challenges of the Internet while also posing some new ones.

8.4.1.1 End-to-end security

As defined by Cisco, an end-to-end security system is a non-negotiable absolute prerequisite needed to achieve a secure communication process [25]. It entails keeping a layer of protection over the data transmitted from one end of the communication to the other without creating a chance of being read, eavesdropped on, tampered with or intercepted by unauthorized users. End-to-end security has been a major challenge for many devices in IoT and their applications. With the heterogeneous architecture and the number of devices that all are connected for

information sharing and collaboration, there is a serious security challenge posed to end-to-end security. It becomes a lot more difficult to create secure communication when the devices possess varying attributes and employ different communication protocols (e.g., 802.11 vs. 802.15.4).

Again, most of the devices in the IoT have unequal capabilities. The majority of computers, smartphones and various types of computerized devices establish a connection with the Internet via HTTP, SMTP to carry out a lot of their actions, thereby using TLS and IPsec protocols for dynamic negotiation of session keys, and creating a level of security. But many other devices in the IoT cannot support these protocols as a result of their limitations in computing and power capacity. Also, embedded devices in the IoT may not have to use HTTP or IP for communicating, thus having limited connectivity.

8.4.1.2 Data security

Data security covers the protocols in place for protecting data during storage and communication. As defined by [26], data security involves putting measures in place to prevent unauthorized access to data by destructive bodies. In other terms, is referred to as information security, data security is very essential to the security of IoT and closely linked to its safety. Conventionally, the effect of breaches in the security of data has been confined within the scope of hacks of user personal information or uncensored access to critical information, e.g., financial information. But in recent times, these breaches could threaten the safety of humans. A major example is when unauthorized access to information transmitted from and to a self-driving car or a heart pacemaker could lead to a critical threat to the life of the user. In another view, when a breach occurs in an IoT-enabled forest fire detection system, the resulting event would be catastrophic.

8.4.1.3 Identity and access management

Cases of identity theft, impersonation, access credentials forgery, masquerading are examples of types of security attacks that face identity protection in IoT. The mechanism by which identification, representation, searching and accessing of things in IoT remain a mystery, thus, leaves devices vulnerable to attacks on their identity. There have been instances where a device in the IoT utilizes fake identities to gain access to services and information provided by another IoT device, a process referred to as a masquerade attack. In many cases, devices have to employ mechanisms with stricter and secure algorithms to be able to detect unauthorized access being sought by devices, thereby detecting imposters on short notice. Attacks that are targeted toward IoT include Spoofing, Masquerade, MiM and Smurf attacks.

8.4.1.4 Compliance

When preserving security in IoT systems, ensuring strict compliance with laid down government laws and regulations guiding the industry is an important factor to note. Devices that are interconnected in the IoT must ensure that they adhere to the necessary privacy policies and protection laws since IoT revolves around

communication done autonomously by devices. This emphasizes the need to ensure adequate privacy and security.

8.4.1.5 Physical and DoS security risks

In conventional network devices, there are certain protection measures put in place to combat physical attacks or malicious access, for instance, securely storing routers in cabinets. Also, in IoT, the interconnected devices would need to have some form of protection mechanisms against attacks. Thus, implementing the physical security of devices is a vital consideration in IoT. In addition, denial of service (DoS) attacks are common in IoT. In its full activity, a typical DoS attack prevents the authorized users from getting access to the services of a server by bombarding the server with illegitimate service requests in a bid to fully exhaust the computational power of such server [27]. This possibility of experiencing DoS attacks also extends to WSNs.

Furthermore, the IoT, being heterogeneous in model and employing complex communications protocols, has an increased vulnerability to a distributed denial of service (DDoS) attack. The DDoS is a form of attack formulated by several agents in the network and initiated from different locations [28]. This makes such disruptive attacks, DoS and DDoS attacks a very great risk to the IoT as a lot of the devices have limited power, memory and processing abilities and can easily get all their available resources exhausted by a well-targeted attack [29].

In an attempt to counter DoS attacks, some protocols required the address of an initiating host to be verified before requests are responded to. Such protocols include DTLS, IKEv2, HIP and Diet HIP [29]. Other methods for creating resistance to DoS attacks include employing clustering techniques to detect DoS attacks in WSNs [30]. Other solutions revolved around designing intrusion detection systems, which could work specifically for WSNs [31].

8.4.2 IoT new security challenges

In IoT, fundamental issues of security, including authorization, authentication, integrity, trust and confidentiality are necessary to be tackled. But this security is often a challenge due to the unavailability of security protocols and infrastructure. This creates a lot of new security issues that are often more severe than the existing security challenges in the system.

The new security issues stem from the structure of IoT that is dynamic, the multiple forms of communication that are embedded and the properties of the devices that tend to make them low-cost. This reveals that these security challenges cannot be tackled using the existing security solutions since the architecture of modern IoT varies from that of the conventional Internet. With the continuous evolution of IoT and its ever-increasing complexity, there is also an increase in the complexity of these security challenges which is linked to two basic factors: low cost and heterogeneity.

With low cost, there is an increasing trend for large-scale deployment of IoT devices that have several constraints in their resources with devices having low-power capabilities, limited memory resources and inadequate computational

abilities [32]. For instance, in a bid to implement some of the conventional Internet security techniques, such as public key infrastructure (PKI) and certificate authority (CA), the cost of IoT devices increases. When considering heterogeneity, diverse devices and communication protocols in IoT raise the amount and degree of complexity of security challenges. For instance, when WSNs are integrated into the Internet, newer security issues are created from the connection of the sensor node to the Internet device. In a more practical implementation of using communication devices having low power, such as ZigBee or IEEE 802.11ah, there is a need to create a link for secured communication with a high-power device like a smartphone and this requires employing necessary cryptographic techniques without utilizing a lot of energy and bandwidth. This becomes an additional feature to the basic security protocols already employed in establishing a secured connection to the Internet.

8.4.3 IoT security requirements

Authorization: In many smart IoT devices, conventional authorization techniques are used to satisfy this requirement. An administrator could be assigned to block unauthorized access in low-power devices such as ZigBee IP. This prevents these unauthorized requests from being routed to IoT devices.

Authentication: Authentication is a process that involves the verification of the identity of someone requesting access. This is mostly done by employing a username and password-based authentication protocol. However, this system has been proven not to have enough security as passwords usually require them to be changed frequently and also they cannot be used without keeping close attention to the device on which they are being used. Now, the Secure Sockets Layer protocol is commonly being used for authentication by websites. The process of authentication also involves requesting both senders and receivers to verify the origin of the information they are exchanging. This requirement is quite complex to satisfy as the things in the IoT may not have a dedicated IP address.

Integrity and freshness: Message integrity tries to ensure that messages have not been altered in any way. This is a very important requirement because IoT is all about information being transmitted to perform a particular operation. Freshness helps to ensure that only fresh messages are transmitted and not older messages being replayed.

Confidentiality: IoT must ensure that the personal and sensitive information of users is protected from unauthorized access by malicious entities.

Resilience to attacks: An IoT system must have the self-recovery capability in the advent of a crash. For instance, a server that works in an environment with multiple users must have enough intelligence and strength to protect itself from entities who might try to intrude or eavesdrop. In such a scenario, when it goes down, it would perform a self-recovery without users being conscious of its downtime conditions.

8.5 Privacy

IoT devices create links with insignificant strength that could be exploited by malicious entities and lead to events of a high volume of surveillance, tracing,

tracking and monitoring of the activities and movements of users. This is due to the nature of the devices being distributed in large volumes [33]. Nowadays, several privacy threats are being introduced as a result of the proliferation of mobile devices, GPS devices and other modern technologies in humans. For example, the study in [34] revealed that the home location of a driver could be deciphered from the GPS information retrieved from his vehicle. Further revelation explains that the outer of an individual could be reconstructed so as to cater for the provision of a detailed profile of his movement that could enable interference. Another example is the indication of illness by recurring visits to a medical clinic, and consistent visits to activist organizations could signal political ideas [35]. This marks an indication that privacy incidents could have reasons to be on the increase as IoT continually finds expression in our everyday lives. Thus, privacy is fast becoming one of the major concerns as IoT undergoes increasing development.

In IoT, privacy is no longer being defined by anonymity [28]. Cases of profiling and mining of data in an IoT situation could lead to danger to the users as a result of data being collected and stored automatically, and the easy means of sharing and analyzing personal data. One interesting potential carried by IoT is the capability for devices to autonomously communicate with their environments by sensing and observations. This causes attackers to configure devices with an ability to autonomously carry out information retrieval about the environment of the system or the user in view [36]. The most pressing concern with devices in IoT is their autonomous exchanging of information between themselves. Another source of risk and vulnerability to user privacy are devices that are capable of logging data about their environment. This risk becomes a reality, especially the leakage of information when the devices begin to share data logs amongst themselves [37].

The enormous volume of data, belonging to a wide range of owners, including users, organizations and the general public, has been made available by the IoT [38], which could be a pointer to particular interests, destinations and intentions [39]. Although the opportunities provided are great, in terms of improving the quality of services, this must be considered also but not to jettison privacy preference. Users must have a level of trust in the services they use when putting regards to their privacy. Trust becomes a fundamental factor for users to consider while adopting new technology [40]. This is reflected in the reluctance of users to employ new technologies if there is not enough trust developed as regards their privacy, security and safety, which is more pronounced in the IoT [41,42].

A varying collection of data about users is retrieved by sensors, which then undergoes aggregation, analysis, processing, fusing and mining to allow the extraction of vital information for assistance in intelligent operations [43]. In 2006, Barnes [44] proposed a privacy paradox in which it stated that "adults are more worried about their privacy intrusion, while on the other hand teens tend to release information freely." In the year 2010, Mark Zuckerberg, the Facebook founder, justified the change in the default privacy setting by saying that "privacy is no longer a social norm," though this has been subjected to lengthy debates by academics.

Recently, in the report released by the Oxford Internet Institute, a new privacy paradox was proposed by [45] in which it was argued that younger people have a

higher tendency to take definite actions to protect their privacy than older people. A more recent study carried out by Pew Research Center [46] revealed that 86% of the users of Internet services would have at a point taken deliberate actions to remove or cover their online tracks. Some of the actions taken include cookies clearing, employing pseudo-names, encryption of emails and hiding their IP addresses using virtual networks.

In distributed systems, one way of ensuring that trust is developed is by allowing users have more control over how their personal information is collected [35]. In previous projects, like the Platform for Privacy Preferences Project (P3P), users were given controlling access when the web browsers are being used. The P3P protocol, which was initiated by the World Wide Web Consortium in 2002, ensures that websites openly state their intention in the usage of information that is collected via their web browsers [47]. This is as a result of trying to translate website privacy policies into some form of information that could be read by the machine to enhance transparency and give users the opportunity to choose [48]. Although the project had to end prematurely, it had experienced some level of implementation [35].

8.5.1 Consent

As mentioned in the previous section, it is vital to create a balance between service optimization and personalization with privacy preference. One technique that could be adopted to attain this balance is to create an environment where users give consent for the collection, storage and sharing of data. But this creates another set of challenges. Traditionally, consent has been based on a transparent system in which the service provider explicitly states the kind, amount and use of the data being collected. Although there have been a lot of deliberations on the concept of having to present a user with numerous pages of details, various challenges are associated with the non-provision of an adequate interface on web pages to either offer or retract consent. These challenges do not only come to play in public places but also occur at homes that have embedded systems running IoT. An example is sensitive data retrieved from the pressure sensors, IR sensors, and RFID systems form enough source of information for monitoring and understanding the activities of humans in a home. A practical example is personal data that are retrieved from an IoT-enabled fridge that could be employed to predict the eating habits and the health conditions of the user, which might have an effect on the insurance policy with an insurance firm.

Privacy concerns related to the IoT also have effects in the industrial setting. With the enormous complexity of the industrial IoT than traditional ICT systems, there exists the potential for large-scale attacks as a result of its large attack surface with numerous potential attackers [49]. Thus, there needs to be a formulation of privacy requirements to prevent danger [50]. Looking beyond the risk of sensitive information of employees or clients being violated, the tendency to lose intellectual properties creates an avenue for competitors to reproduce the knowledge and the products of such an organization, leading to a potential loss of competitive advantage [49]. Although cases of industrial espionage could lead to theft of

intellectual properties, compromising privacy could result in this intellectual capital leakage. For instance, if an event of data involving industrial orders is compromised, it could help the competitor in predicting the current state of goods and materials, and the futuristic supplies and innovations that are being developed. In another vein, when data protection is compromised, the financial performance and strength, together with the intellectual capacity of the industry, could be revealed, which could lead to severe financial implications in the long run.

8.6 Conclusion and future scope

Despite the fact that security and privacy issues have become key issues in our present world, the importance of incorporating IoT into our healthcare system cannot be overemphasized, as this will make healthcare accessible to more citizens especially those residing in the rural areas of the developing countries. Though there is a need to always create layers of security whenever IoT is being incorporated into our healthcare system in order not to compromise the patient's records.

References

[1] K. R. Darshan and K. R. Anandakumar, "A Comprehensive Review on Usage of Internet of Things (IoT) in Healthcare System," in *International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, India, 2015.

[2] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[3] R. K. Kodali, G. Swamy and B. Lakshmi, "An Implementation of IoT for Healthcare," in *IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, Trivandrum, India, 2015.

[4] J. Gómez, J. F. Huete, O. Hoyos, L. Perez and D. Grigori, "Interaction System Based on Internet of Things as Support for Education," *Procedia Computer Science*, vol. 21, pp. 132–139, 2013.

[5] N. I. Council, "Disruptive Technologies Global Trends 2025. Six Technologies With Potential Impacts on the US Interests Out to 2025," 2008.

[6] K. K. Raghavendra, P. S. Sharanya and P. Shaila, "An IoT Based Smart Healthcare System Using Raspberry Pi," *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 5, no. 6, 2018.

[7] S. K. Dhar, S. S. Bhunia and N. Mukherjee, "Interference Aware Scheduling of Sensors in IoT Enabled Health-Care Monitoring System," in *4th International Conference of Emerging Applications of Information Technology*, Kolkata, India, 2014.

[8] J. Gomez, B. Oviedo and E. Zhumab, "Patient Monitoring System Based on Internet of Things," *Procedia Computer Science*, vol. 83, pp. 90–97, 2016.

[9] M. Swan, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self," *Journal of Sensor and Actuator Networks*, vol. 1, no. 3, pp. 217–253, 2012.
[10] V. Prajoona, A. Tariq and H. Ali, "IoT Based Health Monitoring System," *Journal of Critical Reviews*, vol. 7, no. 4, pp. 739–743, 2020.
[11] R. M. Gardner and M. Shabot, "Patient-Monitoring Systems," in *Decision Support Systems in Critical Care*, Boston, Springer-Verlag, 1994.
[12] V. Shnayder, B. Chen, K. Lorincz, T. R. F. Fulford-Jones and M. Welsh, "Sensor Networks for Medical Care," in *3rd International Conference on Embedded Networked Sensor Systems*, New York, USA, 2005.
[13] S. Naddeo, L. Verde, M. Forastiere, G. De Pietro and G. Sannino, "A Real-Time m-Health Monitoring System: An Integrated Solution Combining the Use of Several Wearable Sensors and Mobile Devices," 2017.
[14] World Health Organization, "Chronic Diseases and Health Promotion," 2016.
[15] N. Townsend, L. Wilson, P. Bhatnagar, K. Wickramasinghe, M. Rayner and M. Nichols, "Cardiovascular Disease in Europe: Epidemiological Update 2016," *European Heart Journal*, p. 334, 2016.
[16] D. Niewolny, "How the Internet of Things Is Revolutionizing Healthcare, Freescale Semiconductors," 2013.
[17] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.
[18] Y. J. Fan, Y. H. Yin, L. Da Xu, Y. Zeng and F. Wu, "IoT-Based Smart Rehabilitation System," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1568–1577, 2014.
[19] C. Rotariu and V. Manta, "Wireless System for Remote Monitoring of Oxygen Saturation and Heart Rate," in *Federated Conference on Computer Science and Information Systems (FedCSIS)*, Wroclaw, Poland, 2012.
[20] L. Yang, Y. Ge, W. Li, W. Rao and W. Shen, "A Home Mobile Healthcare System for Wheelchair Users," in *IEEE International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Hsinchu, China, 2014.
[21] C. Lee, "MS Mobile Devices and Apps for Health Care Professionals: Uses and Benefits," 2014.
[22] M. Elkhodr, S. Shahrestani and H. Cheung, "A Semantic Obfuscation Technique for the Internet of Things," in *IEEE International Conference on Communications (ICC)*, Sydney, Australia, 2014.
[23] A. Darwish and A. E. Hassanien, "Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring," *Sensors*, vol. 12, pp. 12375–12376, 2012.
[24] H. Alemdar and C. Ersoy, "Wireless Sensor Networks for Healthcare: A Survey," *Computer Networks*, vol. 54, pp. 2688–2710, 2010.
[25] M. H. Behringer, "End-to-End Security," *The Internet Protocol Journal*, vol. 12, p. 20, 2009.

[26] G. Summers, "Data and Databases," in *Developing Databases With Access*, Nelson Australia Pry Limited, 2004, pp. 4–5.

[27] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defence Mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39–53, 2004.

[28] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena and M. S. Obaidat, "A Learning Automata-Based Solution for Preventing Distributed Denial of Service in the Internet of Things," in *2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, 2011.

[29] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar and K. Wehrle, "Security Challenges in the IP-Based Internet of Things," *Wireless Personal Communications*, vol. 61, pp. 527–542, 2011.

[30] D. Mansouri, L. Mokdad, J. Ben-Othman and M. Ioualalen, "Detecting DoS Attacks in WSN Based on Clustering Technique," in *Wireless Communications and Networking Conference (WCNC)*, 2013.

[31] D. Martynov, J. Roman, S. Vaidya and H. Fu, "Design and Implementation of an Intrusion Detection System for Wireless Sensor Networks," in *IEEE International Conference on Electro/Information Technology*, 2007.

[32] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, pp. 51–58, 2011.

[33] M. Elkhodr, S. Shahrestani and H. Cheung, "The Internet of Things: Vision & Challenges," in *IEEE Tencon Spring 2013*, Sydney, Australia, 2013.

[34] B. Hoh, M. Gruteser, H. Xiong and A. Alrabady, "Enhancing Security and Privacy in Traffic Monitoring," *IEEE Pervasive Computing*, vol. 5, pp. 38–46, 2006.

[35] P. Beatty, I. Reay, S. Dick and J. Miller, "P3P Adoption on e-Commerce Web Sites: A Survey and Analysis," *IEEE Internet Computing*, vol. 11, no. 2, pp. 65–71, 2007.

[36] S. Sicari, R. Alessandra, A. G. Luigi and C.-P. Alberto, "Security, Privacy and Trust in the Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[37] J. H. Ziegeldorf, O. G. M. Morchon and K. Wehrle, "Privacy in the Internet of Things: Threats and Challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[38] D. Gessner, A. Oliveira, A. S. Segura and A. Serbanati, "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things," in *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Liverpool, England, 2012.

[39] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things (IoT)," *IEEE Computer*, vol. 44, pp. 51–58, 2011.

[40] Z. Yan, P. Zhang and A. V. Vasilakos, "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[41] M. Taddeo and L. Floridi, "The Case for E-Trust," *Ethics and Information Technology*, vol. 13, pp. 1–3, 2011.
[42] I. W. Foundation, "Maximize Insight, Ensure Trust and Improve IT Economics – United States," 2015.
[43] Z. Yan and S. Holtmanns, "Trust Modeling and Management: From Social Trust to Digital Trust," in *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, Hershey, PA, IGI Global, 2008.
[44] S. B. Barnes, "A Privacy Paradox: Social Networking in the United States," *First Monday*, vol. 11, no. 9, 2006.
[45] G. Blank, G. Bolsover and E. Dubois, "A New Privacy Paradox: Young People and Privacy on Social Network Sites," in *American Sociological Association Annual Meeting*, San Francisco, CA, 2014.
[46] L. Rainie, S. Kiesler, R. Kang, *et al.*, *Anonymity, Privacy, and Security Online*, Pew Research Center, Washington, DC, 2013.
[47] L. F. Cranor, S. Egelman, S. Sheng, A. M. McDonald and A. Chowdhury, "P3P Deployment on Websites," *Electronic Commerce Research and Applications*, vol. 7, no. 3, pp. 274–293, 2008.
[48] A. Jøsang, L. Fritsch and T. Mahler, "Privacy Policy Referencing," in *International Conference on Trust, Privacy and Security in Digital Business*, Bilbao, Spain, 2010.
[49] A.-R. Sadeghi, C. Wachsmann and M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," in *52nd ACM/EDAC/IEEE Design Automation Conference*, San Francisco, CA, 2015.
[50] L. Da Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.