# Chapter 6
# Networking and Security Architectures for IoE Networks


**Fasee Ullah and Asad Ullah**

## 6.1 Overview

For this decay, the Internet of Everything (IoE) is the underlying super network architecture and sub-class of the existing Internet of Things (IoT). This chapter broadens the reader's knowledge and piques their interest in emerging IoE networks. The chapter is broadly categorized into two main streams including securing the IoE by using advanced wire and wireless-based architecture and securing by using advanced digital image processing. The main objective of this chapter is to explore the network and security architecture for IoE networks. The importance of this research is to improve the IoE network and device security, which is necessary for the broad adoption of these technologies. Utilizing cutting-edge methods and cybersecurity precautions will assist in avoiding cyberattacks, safeguarding sensitive data, and guaranteeing the secure and dependable operation of IoE networks. We encourage more research to develop more sophisticated techniques because this study shows the potential of DIP and advanced cybersecurity measures in boosting the security of IoE devices and networks.

F. Ullah (✉)
Computer and Information Sciences Department, Universiti Teknologi Petronas, Perak Darul Ridzuan, Malaysia

A. Ullah
Department of CSE, Military College of signals, NUST, Islamabad, Pakistan
e-mail: asadullah@mcs.nust.edu.pk



K. Naseer Qureshi et al. (eds.), *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Internet of Things,
https://doi.org/10.1007/978-3-031-45162-1_6

## 6.2 Internet of Everything

The IoT networks are based on two terms: Internet and things. The Internet means connecting local devices by using wired or wireless networks for data sharing, and things are devices and human beings. Moreover, the IoE is an extension of IoT and was introduced by Cisco in 2013 [1]. IoE aims to make the Internet smarter by connecting complex dimensions of existing objects and artificial intelligence (AI)-based future objects. The examples of IoE applications are starting from home to commercial sectors such as transportation (railway, airlines, ships, vehicles), small and large machines, humans, and home and office appliances [2]. Thus, IoE networks connect the living things and non-living things of the world and generate heterogeneous data due to different data traffic with different generation rates.

The IoE network is a fast-developing technology, where billions of devices are connected electronically. This is a developing technology that connects billions of things, such as industrial machinery, cell phones, and sensors, to the Internet. The IoE can revolutionize several industries, including healthcare, transportation, and manufacturing, by enabling real-time equipment and process monitoring, analysis, and management [3]. These networks are based on smart and intelligent systems to facilitate the users. However, there are serious cybersecurity risks associated with this interconnectedness. The threat of cyberattacks, which can result in data theft, device malfunction, and even physical harm to people, is growing along with the number of connected gadgets. Establishing strong cybersecurity measures is crucial for the security of IoE devices and networks [4].

IoE devices and networks are vulnerable to cyberattacks because of their interconnectedness, including denial of service (DoS) attacks, port scans, malware attacks, and phishing efforts. The diversity of IoE devices and networks, the vast amount of data created by IoE devices, and the dynamic nature of network settings may make conventional cybersecurity solutions insufficient to safeguard devices and networks. As a result, there is a need for new and cutting-edge cybersecurity techniques that can adjust to the particulars for IoE networks. The IoE networks can also be secured by using cutting-edge cybersecurity methods, including intrusion detection systems (IDS), firewalls, and access control systems.

## 6.3 Pillars of IoE

IoE is the super extension of the IoT, and its existence is based on the four pillars of people, things, data, and process [5]. People are a critical part of IoE, which is connected to the Internet through intelligent digital devices like computers, smartwatches, and other gadgets. These devices produce data through user interaction, and users can analyze it through websites, intelligent applications, and social networking. In smart healthcare systems, the analogy of the people and their vital signs are monitored by using smart sensor nodes which forward the sensory data with the

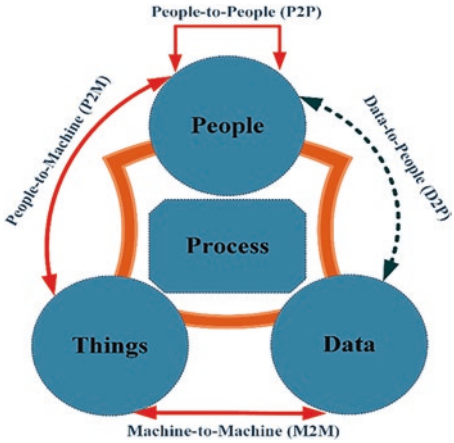


**Fig. 6.1** Typical overview of Internet of Everything (IoE)

help of base station (BS) to the medical team for optimal suggestion and treatment. Moreover, the monitored vital signs of the patient's body are used to detect any abnormality in terms of low threshold or high threshold values.

Thus, people are considered to solve the problems by making different decisions to understand the choirs level of the different business groups. This whole process is situated in the people-to-people (P2P) category of the IoE environment. Furthermore, smart physical devices take instructions from people and those who interact with them through intelligent web applications. The interaction connection between people-to-machine (P2M) generated a huge volume of data to establish thoughtful and intelligent business decisions at the right time for better opportunities. The physical devices generated raw data that can be used for decision-making.

The existing IoT-based industries use AI methods with machine learning (ML) and federated learning algorithms to extract the features from gathered data and process and analyze it for better decision-making. This perfect decision process ensures customer satisfaction to grow the business networks of an organization. Figure 6.1 shows the typical overview of the main pillars of IoE networks including the processing module, which is the critical feature in gathering, analyzing, and processing data from different sources with the intervention of the people, data, and things.

## 6.4 Proposed Security Architecture for IoE Networks

IoE networks build relationships with social networks as a service-distributed architecture by connecting multiple devices and proposing services or protocols to other devices for different activities. In service-distributed architecture, we must design and develop a trust management system that establishes relationships between IoE

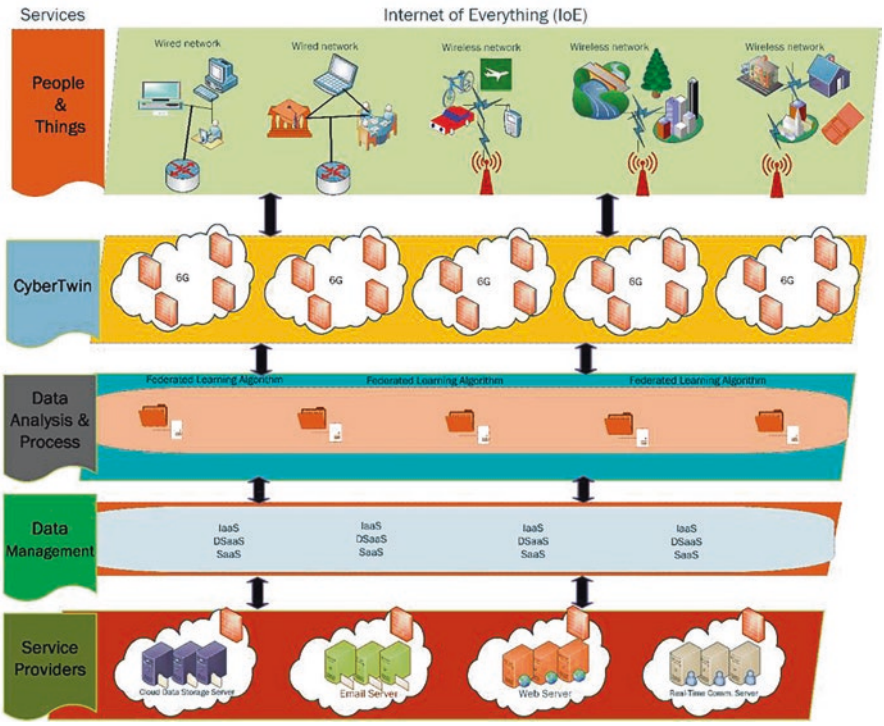


**Fig. 6.2** Proposed security architecture for IoE network

devices. This section proposed a security architecture for IoE networks, comprising every living and non-living object and placing them into the people and things categories. The things or objects are computers, smartphones, and human beings which are connected by using wired and wireless-based networks through fiber optics and Wi-Fi technologies. Figure 6.2 shows the proposed security architecture for IoE networks.

Furthermore, these networks forward the data requests to the concerned servers to avail services, and the request of each object is verified for security issues using CyberTwin infrastructure. CyberTwin is the security authenticator server containing various filtering options by providing confidentiality, integrity, and availability (CIA) services. Next are the data analysis and process management services containing various machine learning algorithms. For instance, the federated learning algorithm extracts various required features in a distributed manner after clearing the security threats like spam, virus, or other attacks. Moreover, IaaS (Infrastructure as a Service), DSaaS (Data Science as a Service), and Software as a Service (SaaS) provide different types of required platforms for the required data and operations accordingly. We need different hardware and software services to allocate based on different user requests. The final part of the IoE network is the network service providers, including a cloud data storage server (CDSS), email server (ES), web server (WS), and real-time communication server (RTCS).

### 6.4.1 *Advanced Wire- and Wireless-Based Technologies for IoE Security Architecture*

The IoE network comprises different devices which are connected for sharing resources in the network. These networks are organized by using different technologies and standards and are further connected to other networks internally or externally for sharing the network resources. These networks are connected to different city and country networks and are called networking or inter-networking. Such examples of inter-networking are smart education, smart healthcare, smart intelligent transportation systems, smart agriculture, and smart city networks. In education institutes, the students are using Internet services by utilizing the university servers, networks, and local hosting networks. Similarly, the immigration department at the airport checks the travel history and criminal record of the passenger. Figure 6.3 shows the simple network architecture connecting different types of users using web services.

The record is extracted from centralized databases. In smart healthcare applications, a patient needs specific medicines from a particular medicine service provider, and the patient avails the online services to purchase medicines after confirmation from the concerned medical doctor. These various activities generate homogenous data traffic, and the security of the homogenous data traffic networks

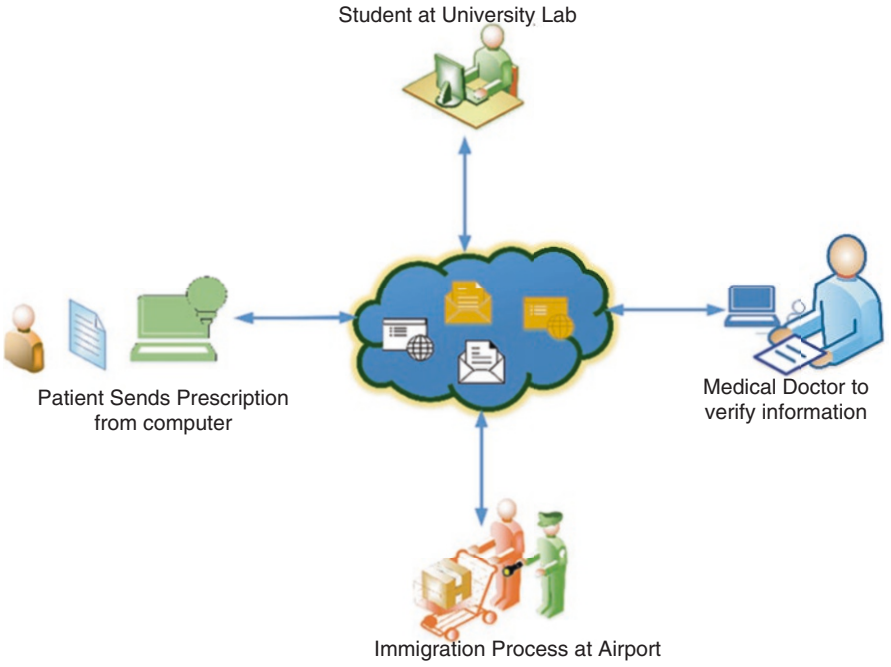


**Fig. 6.3** Wired-based centralized network architecture

is comparatively easy for wireless networks to implement and handle different security threats such as DoS attacks and man-in-the-middle (MITM) attacks [6, 7].

On the other hand, wireless-based networks are used for IoE networks and devices by using different communication technologies and standards. There are different wireless communication standards used such as IEEE 802.15.4 and IEEE 802.15.6. The wireless network is the dominant technology for data transmission without fixing the wire or fixed networks. The wireless-based network architecture transmits the data in the air by using various frequencies.

The sender device generates and transmits data in the air using the registered frequency range. The receiver device (BS) receives the transmitted data and forwards it to the concerned device or network. For instance, different bio-medical sensors in healthcare are employed to monitor different vital signs of a person with three methods of installation/deployment [8, 9].

Smart healthcare technologies are used for elderly aged person home-based monitoring. The injured person who always needs continuous health monitoring or has severe health conditions patients admitted to the Intensive Care Unit (ICU). The first method is to deploy sensor nodes on the patient's body or sewed in the patient's shirt such as electrocardiography (ECG) sensors, blood pressure sensors, and temperature sensors. The second method is to implant the sensors inside the patient's body such as the endoscopy sensor to monitor and analyze different internal organs, such as kidney monitoring, liver monitoring, and taking pictures of the heart from different angles. The third method is to deploy sensors around the patient or around the patient's bed to monitor different physical activities, including sleeping duration and position, detection of the defective sitting position, and fall of the patient. Figure 6.4 shows the basic concept of the deployed IoE devices or sensor nodes for health monitoring.

Tier 1 depicted the sensor nodes or IoE devices placed inside to outside the human body for healthcare purposes. Tier 2 contains a single or multiple BSs to receive the sensory data from the body coordinator (BC), whereas BC collected

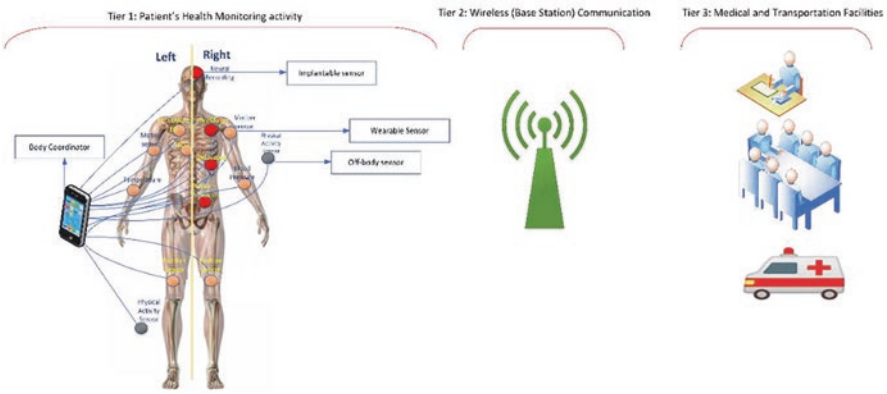


**Fig. 6.4** Overview of the basic concept of the deployed BMSs network for monitoring health

sensory data from the deployed nodes, while Tier 3 contains the medical team, which analyzes the received sensory data based on the patient's medical history and suggests the optimal treatment by responding to the patient.

### 6.4.2 *IEEE 802.15.4 Medium Access Control (MAC) Superframe Structure for Network Communication*

Wireless-based communication standards are used for data communication in IoE networks. This section presents the superframe structures of IEEE 802.15.4 and IEEE 802.15.6 for handling different heterogeneous data in IoE networks. IEEE specified the IEEE 802.15.4 [10] standard for Wireless Sensor Network (WSN) connectivity. In smart healthcare systems, the sensor nodes are implants or attached to patients which track vital signs and are connected to an anatomical interface in a star topology manner [11]. The three types of patient data are regular, periodic, and emergency data. Temperature monitoring is used as normal data, whereas the glucose and blood pressure readings are taken regularly. Life-threatening vital signs are included in the emergency data. In addition, the superframe settings in IEEE 802.15.4 MAC include beacon, CAP (Conflict Progress Period), CFP (Conflict Free Period), and LPL/IP (Low Power Listening/Inactive Period). Every BMS works multiple back-off and precise channel assessments (CCA) to access the channel in contention. Furthermore, the TDMA system access mode is split into CFP slots, and the CFP time allocates the guaranteed time to transmit patient data. In contrast, the body interface allocates CFP access to BMS that received access mode in CAP times. When the sensor nodes are busy sending logical data, IP saves energy. Figure 6.5 shows the IEEE 802.15.4 MAC superframe structure.

The IEEE 802.15.4 MAC superframe configuration has the following limitations.

- The IEEE 802.15.4 superframe structure has a maximum of 16 (0–15) channels.
- During the CAP period, all deployed BMSs compete for channel access.
- Only BMSs with channel access in CAP are assigned CFP channels.

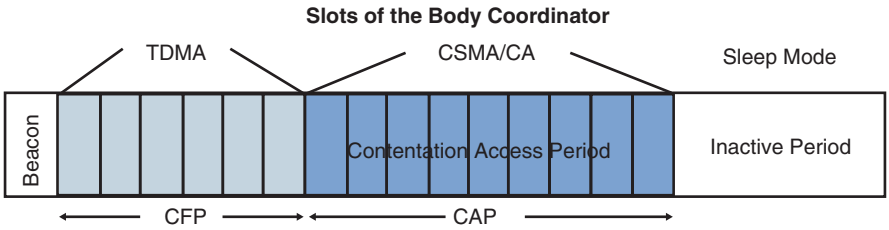


**Fig. 6.5** IEEE 802.15.4 MAC superframe structure

- During channel contention, no priority-based slot is assigned to emergency data. No distinction between normal, periodic, and emergency data is made to assign the first slot based on the priority of the life-critical data.
- BMSs consume more energy and drop patient data if they exceed contention threshold values.

These constraints severely reduce the MAC superframe structure's performance in terms of higher collision; BMSs retransmit the lost data packets, causing a delay with lower reliability and a higher amount of energy consumption, which is unacceptable in an emergency.

### *6.4.3 IEEE 802.15.6 Medium Access Control (MAC) Superframe Structure for Network Communication*

IEEE 802.15 Task Group 6 (TG6) [12] decided to develop low-power sensors for monitoring a patient's critical symptoms and the health situations of athletes in their respective sports. In 2012, the first draught version of IEEE 802.15.6 for the MAC and PHY layers was made public. IEEE 802.15.6, which divides the superframe structure into channels and beacons, is described in this draught version. Each channel is given the same time to transmit the patient's records. The IEEE 802.15.6 MAC superframe shape consists of three major modules: the MAC header, the MAC variable duration, and the Frame Check Sequences (FCS). The MAC header has 7 bytes reserved, the variable duration has 0–255 bytes reserved, and FCS has 2 bytes reserved. Furthermore, the MAC frame body is divided into three sub-headers:

- Data Freshness (one byte) to protect data from reply attacks.
- Message Integrity Code (MIC) occupies 4 bytes to authenticate the frame and maintain the frame's integrity check.
- Data payload contains data in the frame with MIC headers.

Furthermore, the IEEE 802.15.6 MAC header is divided into four sub-headers. First, the Frame Control takes up 4 bytes, distinguishes between the control and data frames, and provides an acknowledgment. The addresses of the receiver and sender sensors are specified in the second and third headers, respectively. Each sensor stores the address in 1 byte. The final header is the body coordinator header, which takes up 1 byte.

#### 6.4.3.1 MAC Superframe Structure of IEEE 802.15.6

The beacon-enabled MAC address, the superframe structure includes a beacon, Exclusive Access Phase (EAP-I–II), Random Access Phase (RAP-I–II), Type (I–II), and CAP periods. The contention-based channel allocation policy for BMSs is

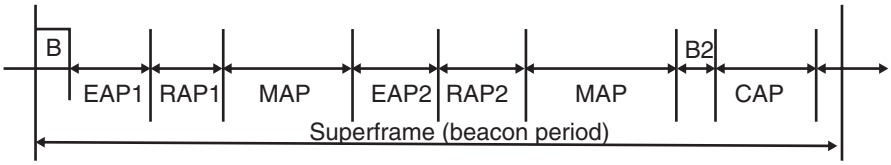


**Fig. 6.6** IEEE 802.15.6 MAC superframe structure

based on CSMA/CA or slotted Aloha schedule access schemes. These access scheduling schemes are used during the EAP, RAP, and CAP periods. Type-I denotes critical data, whereas Type-II denotes non-critical data. However, the limitations of IEEE 802.15.6 MAC Superframe structure are the same as those mentioned in the IEEE 802.15.4 MAC. The non-beacon MAC Superframe structure, on the other hand, allocates the Superframe's entire channels (slots) to the Type-I or Type-II category of a patient's traffic. The disadvantage is that the body coordinator cannot directly transmit data to BMSs but must first send an activation alert signal to the recipient BMS. The non-beacon MAC also allocates slots to one type of patient's data at a time, which is unacceptable in life-critical situations. The third type is the non-beacon without Superframe structure, which uses predefined periods to transmit a patient's Type-II traffic. The slot allocation to BMSs in this Superframe is based on contention or post-contention. The restriction of predefined-based slot allocation to one type of data results in data waste (Fig. 6.6).

## 6.5 Data Collection, Recognition, and Processing in Multiple Environment of IoE

The IoE is an advanced concept of networks that connects multiple nature devices of different networks to collect and exchange data over wired and wireless networks. IoT has the power to receive/collect data, recognize the type of data/network, and process data for various decision-making in a central server/device. For instance, we are presenting a scenario of smart IoT-based health monitoring. There are various data traffics coming from different types of patients, and these various natures of data are called heterogeneous data because each deployed sensor node needs different frequencies or data rates to transmit the data to the designated point. For instance, the heartbeat sensor needs 1.99 kbps, the temperature sensor needs 122 bps, and ECG sensor (12 leads) needs 145 kbps [13]. Collectively, this technology receives data from different critical patients as sensory data for processing. IoE means different sensing data are collected from hundreds of thousands of small devices from multiple sources and are forwarded to the central device. The collected data is raw, and the central device needs to detect, process, and recognize by taking a specific set of actions based on the previous knowledge (using machine learning or deep learning techniques) for optimal decision.

Thus, H-IoEs assume that a patient or person uses different biomedical sensors (BMSs) whose health is monitored frequently. There are other examples like a person who is watching sports activities in the stadium, an ambulance-based patient traveling to the hospital, a person walking and exercising in parks and playgrounds, living in smart apartments, eating in a smart sensing-based restaurant, a person is traveling by a road transport, health is monitored during studies in university, a health condition is measured during sea traveling, and health monitoring of a person during working hours in public offices. Thus, the smart IoE-based sensing devices monitor different vital signs of a patient/person while a person is busy with daily life activities. The centralized server is further categorized into the database server, reasoning rules server, and main server. The database server is a simple data storage server containing the previous knowledge of a patient/person. The reasoning rules server comprises different association rules which fetch the associated data from the database server and applies certain conditions to bring the optimal decision for a patient, accordingly. However, this decision is validated by the domain expert knowledge personnel and forwarded to the central server to store it as the final decision. Figure 6.7 shows the data collection, recognition, and processing in smart healthcare IoE systems.

## 6.6 Diverse Technologies in IoEs

The IoE is a new technology implemented in various data communication environments. Thus, we have broadly classified IoEs as Internet of Ad hoc Network Things (IoAVTs), Internet of Smart Building Things (IoSMTs), and Internet of Underwater Things (IoUTs), with each IoE classified into more than one category of things.

### *6.6.1 Internet of Ad Hoc Network (IoAV)*

The Internet of Ad hoc Network Things (IoAVTs) is a network where communicating objects such as laptops and smartphones are not fixed and stationary. Such devices always move from one location to another without being bound or stuck in one place or location. Furthermore, IoAV devices are outfitted with intelligent sensors and software to connect various things and transmit data gathered from the purpose-built environment over the Internet. Therefore, IoAVTs are divided into four categories: the Internet of Vehicular Ad hoc Networks (IoVAN), the Internet of Mobile Ad hoc Networks (IoMANs), the Internet of Ambulance (IoA), and the Internet of Air Traffic (IoAT).

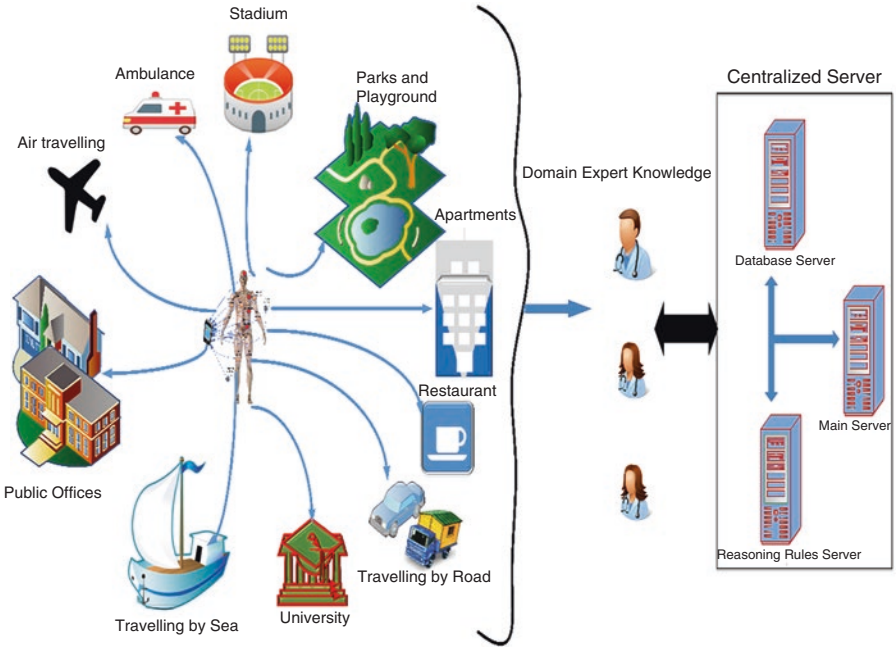


**Fig. 6.7** A smart IoE support-based health monitoring system

### *6.6.2 Internet of Vehicular Ad Hoc Network (IoVAN)*

IoVAN is made up of innovative and intelligent cars that are outfitted with advanced sensing technologies and communicate with other smart cars on the road for vehicle driving and safety. Multiple sites or roads can be outfitted with sensing devices at various points, which should transmit messages about the current state of the location/road, as well as various warning messages, via an agreed-upon standard Internet. In advanced countries, the smart car has a collision warning alert system, issuing alerts on bad driving moods such as overtaking, lousy road or weather conditions, wrong way driving, object (or vehicle) detection on the way, traffic signal and pedestrian walk violation, emergency control breaks, and notification of the hazardous location to the driver's family. Therefore, car-to-car communication should be efficient for the warnings mentioned above for the safety of the car, the people on board, and the best interests of society. Intelligent Transport System (ITS) is another name for IoVAN.

### 6.6.3 Internet of Mobile Ad Hoc Networks (IoMANs)

IoMAN is a network with no fixed infrastructure and consists of a collection of different mobile nodes/sensors connected in an isolated environment for data exchange. IoMANs perform network self-configuration and topology construction based on target/object detection and monitoring. All nodes use wireless channels with different radio frequencies. Furthermore, some nodes are dedicated to stationary monitoring of various activities in IoMANs, while others are regularly placed for movement/mobility monitoring of the targeted object. For example, they are tracking pandas' frequent movement and location in the forest. Thus, stationary nodes send and receive data from mobile nodes of the monitored data over the Internet to the wildlife department to ensure the animals' survival and safety. For data communication in IoMAN, there are two types of communication protocols: proactive and reactive. Proactive protocols calculate and select the best available paths from source to destination before establishing the communication channel. In contrast, the reactive protocol needs to calculate the paths in advance and instead transmits data on-demand without regard for path reliability.

### 6.6.4 Internet of Ambulance (IoA)

The Newport Beach Hospital and Fire Department developed the Simple Triage and Rapid Transport (START) system in 1983. The START system aims to investigate the criticalities of wounded people in mass casualties. On the side of the mass casualties, the paramedic staff arrived by assigning red, yellow, green, and black tags to the wounded to identify criticalities with severe high-risk conditions, wounded by not severe, normal, and dead people, respectively. Based on this information, the ambulance arrives on the scene and transports the injured people to nearby hospitals with available health facilities. The ambulance is equipped with all necessary first aid medication, as well as advanced wireless biomedical sensors that are installed in the ambulance to frequently monitor a patient's survival vital signs such as heart rate, respiratory rate, blood pressure, and temperature. These biomedical sensors are placed on the patient's body and are linked to a central device that collects vital sign readings and sends them to medical doctors. The readings of these vital signs are efficiently and securely transmitted to the nearest hospital's medical doctors, who are ready to treat the patient on an emergency basis.

Furthermore, the vital signs are recorded by a central device placed near the patient, and this device transmits the patient/sensory data to the medical doctors via a dedicated Internet connection. All ambulance cars exchange data on the most direct routes to hospitals while assisting patients with necessary medications. The scenario described above is known as the Internet of Ambulances (IoA). However, an efficient centralized system must be designed and developed to ensure the trust of people using IoA in mass casualties.

### 6.6.5 Internet of Air Traffic (IoAT)

As discussed in IoA, the Internet of Air Traffic (IoAT) is a future network that includes a mini air ambulance equipped with a wireless biomedical sensor to monitor different vital signs of patients in critical health conditions. However, there is a problem with getting patients to hospitals on time in the same city, in different cities, or moving a patient to another country due to heavy traffic or bad weather conditions. It is strongly advised in such cases to transport a patient in critical condition by air ambulance. Furthermore, the medical doctor can remotely operate the patient in an air ambulance using a satellite connection and instructions from other medical doctors. Thus, health treatment services can reduce health risks by fostering trust in IoAT services.

### 6.6.6 Internet of Smart Building (IoSM)

IoSM comprises advanced installed heterogeneous sensor nodes that monitor various activities inside and outside the building, for example, smoke detection inside a room, installed security cameras for surveillance, gas leakage monitoring of pipes deployed inside and outside the building, automatic door opening and closing, and electricity usage monitoring. As a result, we divide IoSM into three categories: Internet of Public Offices (IoPOs), Internet of Smart Restaurants and Hotels (IoRHs), and Internet of Smart Sports Stadiums (IoSSS). IoPO refers to federal and provincial secretariats, law and judiciary offices, post offices, electricity power distribution offices, railway station offices, military/defense offices, hospitals, weather forecasting departments, commerce and textile department, and education. These departments are outfitted with advanced nodes, sensors, actuators, and visual sensors to monitor, detect, and recognize various activities in various departments and report any suspicious activity to the appropriate authority.

The Internet of Smart Restaurants and Hotels (IoRHs) is a collection of networks linked by advanced sensing technologies that detect the mode of the client at a restaurant or hotel and provide services accordingly. Furthermore, different IoRHs are linked to provide different meal and stay services on various occasions, such as Christmas and Chinese New Year. Furthermore, the Internet of Smart Sports Stadiums (IoSSS) is a network of networks outfitted with various sensors to monitor the health of athletes during sports activities. Additionally, visual sensors are deployed around the spectator seating areas to monitor anger situations or anything suspicious and report it to the appropriate personnel. In conclusion, most future IoE networks must design an efficient network architecture without replacing the deployed hardware technologies while ensuring trust and benefits to society's citizens.

### *6.6.7 Internet of Underwater Things (IoUTs)*

The Internet of Underwater Things (IoUTs) is a new innovative framework technology for designing and developing an intelligent communication network for underwater sensors. For data communication, IoUTs employ optical fiber and acoustic signals. Furthermore, the sea is divided into three zones. The first zone is the top surface zone of water, where a base station or wireless antenna is deployed to assist in sending and receiving data from the deep sea. The third zone is the final zone of underwater sensors deployed to monitor, detect, and identify target objects in the sea. It is assumed that the world will face a natural resource shortage after 2050, and thus the only place where the world can collect natural resources from the sea and meet their needs from deep seas, such as meat, salt, copper, gold, chemicals, oil, and gas, is the deep sea. Other advantages include detecting the earth quickly and predicting the effects of shock on the upper level of the sea or earth. Thus, the underwater deployment of sensors would detect various objects, ushering in scientific research and business revolution.

## 6.7 Security in IoE Networks

To safeguard the IoE networks, many cybersecurity measures are considered such as intrusion detection and prevention, access control, authentication, and encryption. To preserve data confidentiality and prevent unauthorized access, encryption method is used. To ensure that only authorized devices and users access the system, authentication entails confirming the identity of both users and devices. Access control entails granting only authorized people and devices access to resources. It entails identifying and responding to security lapses and assaults. The employment of cybersecurity precautions in protecting the IoE has been the subject of several research projects. For instance, authors in [14] proposed a security architecture for the IoE that includes encryption, authentication, and access control mechanisms. A framework for IoE intrusion detection by using ML methods is proposed in [15] and suggested employing encryption and authentication procedures to secure medical images sent over the IoE. Given the IoE's extensive use of various gadgets coupled in complex ways, it faces particular security concerns. These gadgets frequently need higher processing speed and memory due to resource-constraint environment. Traditional security solutions like firewalls and IDS systems become challenging to implement.

### 6.7.1 Intrusion Detection Systems

Discovering unauthorized access to a network or system is known as intrusion detection. Techniques for digital image processing can be used to examine network traffic and spot signs of an assault. For instance, suspicious or odd activity patterns can be found using image filtering. Feature extraction and classification might be utilized to identify particular sorts of attacks, such as denial-of-service attacks or buffer overflow attacks. Software intended to damage a computer system or network is known as malware. Malware can be found using different techniques by observing how a device's software behaves. Image filtering, for instance, can be used to spot malware-indicating patterns of behavior, such as a program that frequently accesses files or sends information to odd places. Using feature extraction and classification is possible to recognize particular kinds of malware, such as viruses, worms, or Trojan horses.

### 6.7.2 Authentication

Verifying a user's or device's identity is the process of authentication. Biometric data, such as fingerprints, facial features, or iris patterns, can be utilized to authenticate persons or devices. For instance, the contrast of an image can be improved via image filtering to make it simpler to distinguish face characteristics. Specific people can be located using feature extraction and categorization and their biometric traits. The IoE offers enormous amounts of data that may be applied to many different purposes but poses security risks. Techniques for digital image processing can be used to extract data from the massive amounts of generated image data, spot anomalies, and spot risks. The IoE can be protected using various cybersecurity techniques, such as encryption, authentication, access control, and intrusion detection. A solid approach to safeguarding the IoE can be achieved by fusing cybersecurity measures with digital image processing techniques.

## 6.8 Proposed DIP Architecture to Secure IoE Networks

There are serious security risks associated with this interconnectedness. The process of hiding information within an image in a way that is unnoticeable to the human eye is known as image steganography. Image steganography can be used in cybersecurity to hide critical information within an image and prevent unauthorized access. Image encryption involves the transformation of an image into a cipher text that cannot be deciphered without a decryption key. Image encryption can be used

in the context of cybersecurity to protect private photographs from unauthorized access. The technique of placing a visible or invisible mark on an image to establish ownership or authenticity is known as image watermarking. Image watermarking can be used in cybersecurity to stop unauthorized usage or distribution of images. Image analysis is the method of dissecting images to find out crucial information. Image analysis can be used to find anomalies or suspicious activities in an image in the context of cybersecurity.

Thus, this study suggests securing IoE using advanced Digital Image Processing (DIP) methods and cybersecurity mechanisms. Additionally, this section examines how DIP can recognize and stop cyberattacks on IoE networks and devices. DIP techniques are used to protect the IoE networks; for instance, authors in [16] suggested an approach for finding anomalies in surveillance photos by combining image processing methods with ML algorithms. A framework for object detection and tracking in surveillance films using deep learning techniques is proposed in [17]. Using image processing methods for intelligent transportation systems, authors in [18] suggested an approach for detecting vehicle license plates.

This section presents the IoE security using advanced DIP methods and cybersecurity mechanisms and how DIP can recognize and stop cyberattacks on IoE networks and devices. By analyzing email headers and message content, DIP techniques can spot phishing attempts, detect malware attacks, and spot patterns of harmful activity in network traffic. The suggested architecture can offer a thorough and integrated approach to protecting IoE devices and networks and can act as a guide for upcoming work in this field [19].

DIP approaches can be used to improve cybersecurity in the IoE, but some obstacles must be resolved. The high computational cost of DIP techniques, which might be a bottleneck for real-time applications, is one of the main problems. Additionally, DIP approaches are susceptible to assaults like adversarial attacks, in which a perpetrator alters an image to avoid detection.

Despite these obstacles, DIP approaches also offer many IoE cybersecurity prospects. DIP approaches can be integrated with other cybersecurity measures like encryption and authentication to provide a more reliable security solution. Using DIP approaches can also enable real-time cyberattack detection and reaction, significantly reducing the effect of a security breach.

This study aims to improve the security of IoE devices and networks by applying cutting-edge DIP techniques and cybersecurity measures. The precise objectives are the following:

1. Analyzing email headers and message content can help spot phishing attempts. DIP techniques can also detect malware attacks and identify harmful behavior patterns in network traffic.
2. To determine if cutting-edge cybersecurity methods, such as intrusion detection systems, firewalls, and access control systems, protect IoE devices and networks.
3. To propose a plan for securing IoE devices and networks by combining DIP methods with sophisticated cybersecurity measures.

4. The use of DIP techniques to detect and stop cyberattacks on IoE networks and devices.
5. The efficiency of cutting-edge cybersecurity solutions, such as firewalls, access control systems, and intrusion detection systems, protects IoE devices and networks.
6. The architecture for safeguarding IoE devices and networks combines DIP approaches and cutting-edge cybersecurity solutions.

The study focuses on utilizing and integrating currently available techniques and measures rather than creating new DIP or cybersecurity measures.

## 6.9 Conclusion

In conclusion, due to the growing number of devices and systems connected to the Internet, protecting the Internet of Everything (IoE) has become a pressing issue. For IoE networks to be protected against cyberattacks and data breaches, advanced digital image processing methods and security structures are crucial. Identifying potential security risks in IoE networks has been proposed using digital image processing techniques, such as object, face, and gesture recognition. To identify unusual behavior or potential security breaches, these algorithms analyze images taken by IoE equipment, such as security cameras. These methods are now more accurate and efficient thanks to the introduction of deep learning algorithms, making them appropriate for usage in practical settings.

The IoE network security also depends on security architectures. These architectures' complete approach to protecting IoE devices and systems includes access control, data encryption, and secure communication protocols. For safeguarding IoE networks, many security designs, including edge computing, fog computing, and blockchain, have been proposed. These architectures make it possible to administer, store, and communicate securely, which increases the security of IoE networks. To stay up with the shifting threat landscape, creating new approaches and structures as IoE networks continue to develop is essential. Modern digital image processing methods and security structures must be used to protect IoE networks from potential security risks. Future research should concentrate on creating more practical and effective methods and structures to improve IoE security.

The IoE network security is a challenging and complex issue, yet cutting-edge digital image processing methods and security designs offer a viable solution to this problem. We can ensure that IoE networks are safe and safeguarded against potential hacker assaults and data breaches by putting these strategies and designs in place.

## References


1. Zou Y, Zhu J, Wang X, Hanzo L (2016) A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE 104 (9):1727–1765. https://doi.org/10.1109/JPROC.2016.2558521
2. ALiero MS, Qureshi KN, Pasha MF, Jeon G (2021) Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services. Environmental Technology & Innovation:101443. https://doi.org/10.1016/j.eti.2021.101443
3. Lakew DS, Dao N-N, Cho S (2022) Adaptive partial offloading and resource harmonization in wireless edge computing-assisted IoE networks. IEEE Transactions on Network Science and Engineering 9 (5):3028–3044. https://doi.org/10.1109/TNSE.2022.3153172
4. Qureshi KN, Alhudhaif A, Haider SW, Majeed S, Jeon G (2022) Secure Data Communication for Wireless Mobile Nodes in Intelligent Transportation Systems. Microprocessors and Microsystems:104501. https://doi.org/10.1016/j.micpro.2022.104501
5. Adhikari M, Munusamy A, Kumar N, Srirama SN (2021) Cybertwin-driven resource provisioning for IoE applications at 6G-enabled edge networks. IEEE Transactions on Industrial Informatics 18 (7):4850–4858. https://doi.org/10.1109/TII.2021.3096672
6. Su J, He S, Wu Y (2022) Features selection and prediction for IoT attacks. High-Confidence Computing 2 (2):100047. https://doi.org/10.1016/j.hcc.2021.100047
7. Qureshi KN, Alhudhaif A, Hussain A, Iqbal S, Jeon G (2021) Trust aware energy management system for smart homes appliances. Computers & Electrical Engineering:107641. https://doi.org/10.1016/j.compeleceng.2021.107641
8. Ullah F, Pun C-M (2022) Enabling Parity Authenticator-Based Public Auditing With Protection of a Valid User Revocation in Cloud. IEEE Transactions on Computational Social Systems. https://doi.org/10.1109/TCSS.2022.3165213
9. Kim J, Caire G, Molisch AF (2015) Quality-aware streaming and scheduling for device-to-device video delivery. IEEE/ACM Transactions on Networking 24 (4):2319–2331. https://doi.org/10.1109/TNET.2015.2452272
10. Thotahewa KMS, Redouté J-M, Yuce MR (2014) Ultra wideband wireless body area networks. Springer,
11. Han W, Wang J, Hou S, Bai T, Jeon G, Rodrigues JJ (2023) An PPG signal and body channel based encryption method for WBANs. Future Generation Computer Systems 141:704–712. https://doi.org/10.1016/j.future.2022.11.020
12. Zhu M, Sui T, Wang R, Sun J (2022) Sensors Scheduling for Remote State Estimation Over an Unslotted CSMA/CA Channel. IEEE Transactions on Network Science and Engineering. https://doi.org/10.1109/TNSE.2022.3210285
13. Sarma J, Biswas R (2023) A power-aware ECG processing node for real-time feature extraction in WBAN. Microprocessors and Microsystems 96:104724. https://doi.org/10.1016/j.micpro.2022.104724
14. Bokhari S, Hamrioui S, Aider M (2022) Cybersecurity strategy under uncertainties for an IoE environment. Journal of Network and Computer Applications 205:103426. https://doi.org/10.1016/j.jnca.2022.103426
15. Magdy M, Hosny KM, Ghali NI, Ghoniemy S (2022) Security of medical images for telemedicine: a systematic review. Multimedia Tools and Applications 81 (18):25101–25145. https://doi.org/10.1007/s11042-022-11956-7
16. Khan SW, Hafeez Q, Khalid MI, Alroobaea R, Hussain S, Iqbal J, Almotiri J, Ullah SS (2022) Anomaly detection in traffic surveillance videos using deep learning. Sensors 22 (17):6563. https://doi.org/10.3390/s22176563

17. Himeur Y, Al-Maadeed S, Kheddar H, Al-Maadeed N, Abualsaud K, Mohamed A, Khattab T (2023) Video surveillance using deep transfer learning and deep domain adaptation: Towards better generalization. Engineering Applications of Artificial Intelligence 119:105698. https://doi.org/10.1016/j.engappai.2022.105698
18. Oliveira-Neto FM, Han LD, Jeong MK (2013) An online self-learning algorithm for license plate matching. IEEE Transactions on intelligent transportation systems 14 (4):1806–1816. https://doi.org/10.1109/TITS.2013.2270107
19. Cai Z, Wan X, Liu X, Ren Q, Lian X, Wang L (2022) Physics-Based Modeling Strategies of Phase-Change Random Access Memory. IEEE Transactions on Electron Devices. https://doi.org/10.1109/TED.2022.3215550