Fault Tolerance and Security Management in IoMT

Rachida Hireche, Houssem Mansouri, and Al-Sakib Khan Pathan

Abstract In recent years, there has been a growing interest in collecting and storing healthcare data which eventually led to a revolution in this field. In fact, the development of IoT-enabled (Internet of Things-enabled) wearable devices like healthcare management software and smart medical sensors has effectively contributed to the rise of this technological revolution. Recently, we have witnessed a trend of increased use of IT (Information Technology) facilities and cyberspace. Cloud computing, which is one of the most significant technologies nowadays, plays a vital role in some mobile healthcare systems. As a result, it is highly expected that this trend would develop fast in the coming days and contribute to the field of IoMT (Internet of Medical Things) as a whole. In fact, the necessity of IoMT for remote healthcare services has significantly been realized during the recent outbreak of COVID-19 pandemic. Due to the prominent role and importance of IoMT, it is quite evident that such systems should be well protected and supported through efficient fault tolerant mechanisms and security mechanisms. In this chapter, we would explore the fault tolerance issues in such complex healthcare setting alongside the security assurance issues.

Keywords Fault tolerance · Healthcare · IoMT · IoT · Security management

R. Hireche (✉) · H. Mansouri
Laboratory of Networks & Distributed Systems, Computer Science Depart-Ment, Faculty of Sciences, Ferhat Abbas Setif University 1, Setif, Algeria
e-mail: hireche.rachida@univ-setif.dz

H. Mansouri
e-mail: mansouri_houssem@univ-setif.dz

A.-S. K. Pathan
Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh

A. K. Pathan (ed.), *Towards a Wireless Connected World: Achievements and New Technologies*, https://doi.org/10.1007/978-3-031-04321-5_4

1 Introduction

Nowadays, Internet of Medical Things (IoMT) has become a building block for modern healthcare as it is able to operate with significantly stringent resources. Over the course of last two decades, it has been greatly enhanced to be used by healthcare providers for different purposes within this field: improving quality of treatments, managing diseases, reducing errors, improving patient experience, managing drugs, and even lowering costs. However, these applications are often prone to serious security issues which is a major impediment to the evolution and rapid deployment of this sophisticated technology. Issues related to this include mainly: identity theft, information theft, and data modification. In fact, these security problems represent real danger for the IoMT environment as medical data are often considered personal and sensitive.

One of the prominent cases of DDoS (Distributed Denial-of-Service) attacks took place in October 2016, which was launched on DNS (Domain Name System) service provider through an IoT botnet. The botnet used a malware named *Mirai*. The latter led to shutdown of huge portions of the Internet including Twitter, the Guardian, Netflix, Reddit, and CNN [1].

With the fact that such dangerous threats could be active at any point of time, the need arises for strong security mechanisms to protect the IoMT infrastructure. As we know, the first step to ensure security, which is a critical factor, is the complete understanding and appropriate categorization of existing and potential threats to the IoMT environment. It has been shown through several on-going research works that the implementation of secure IoMT applications is achievable by incorporating security measures with each involved technology. Moreover, the development of new IoMT technologies combined with Artificial Intelligence (AI), Big Data and Blockchain offers a variety of possible solutions [2]. The aim of this chapter is to study the existing literature and identify the factors and obstacles affecting the expected development of IoMT and its wide-spread use.

Following the Introduction, the rest of the chapter includes the following:

- In Sect. 2, we present the context of IoMT systems and their architecture, we specify the security requirements of IoMT systems, and also consider the current security techniques and their robustness against various existing attacks.
- In Sect. 3, we discuss different attacks against the IoMT system and classify the security techniques discussed to prevent or mitigate these attacks.
- In Sect. 4, we present for each layer of the IoMT system, the communication protocols and mechanisms used in different medical devices within the healthcare ecosystem. We also discuss the level of security for each mechanism studied as well as possible mitigation solutions.
- We conclude the chapter in Sect. 5 with some future research directions.

2 Internet of Medical Things (IoMT)

In order to understand the later sections, this section presents a general overview of IoMT systems, their architecture, the different security requirements as well as the available security techniques.

2.1 IoT and IoMT

The term, Internet of Things (IoT) refers to a wide range of interrelated objects and devices which use embedded systems like processors and sensors to collect information from the environment. After harvesting data, these devices analyze that. Then, through actuators, they act back and take action on the physical world [3]. By integrating every object for interaction through embedded systems, IoT enhances the ubiquity of the Internet. This leads to a highly distributed network of devices that can communicate with other devices and human beings [4].

Nowadays, the field of healthcare is witnessing a remarkable development thanks to the Internet of Things (IoT). With the ongoing development of different IoT technologies such as smart sensors and advanced lightweight communication protocols, it has been possible to interconnect many medical "*things*" to monitor and examine biomedical signals. Moreover, these IoT devices can even diagnose different diseases without any human intervention and thus they are called Internet of Medical Things (IoMT) [5]. Therefore, we can conclude that IoMT is mainly a network of devices which is connected to the Internet that uses sensors and electronic circuits to collect data in the form of biomedical signals from a patient [6]. Then, a processing unit processes these biomedical signals, a network device transmits the collected data over a network, a permanent or temporary storage unit is used to store data, and finally, a visualization platform is used with artificial intelligence schemes, so that it is capable of making decisions at the convenience of the physician.

2.2 Types of IoMT Devices

IoMT systems provide either needed or enhanced assistance for many medical conditions. Consequently, they can be classified into two main categories: Implantable Medical Devices (IMDs) which are necessary devices for specific medical conditions like pacemakers, and the Internet of Wearable Devices (IoWD) which are assistive devices to enhance the healthcare experience like smart watches.

Implantable Medical Devices (IMDs). As the name suggests, an Implantable Medical Device (IMD) is a device which is implanted to replace a missing biological structure or to support a damaged biological structure. Moreover, an IMD can even be used to enhance an existing biological structure. The main purpose of such

implantable devices is monitoring signals from the patient's body and to send them to other medical systems [7]. They are mainly made up of tiny wireless modules and health sensors that collect like temperature, motion blood glucose and blood pressure. An example of such IMDs is the pacemaker which can be very useful for controlling abnormal heart rhythms. If the heart ever beats too fast or too slow from its normal rate, the pacemaker will work in an effective way to bring back the heart to its normal rate [8]. To keep such kind of devices in the human body for a long time, there are certain requirements for the IMD. Some of these requirements include low power consumption and small batteries that last a long time. The typical lifetime of a pacemaker, for example, is determined by how frequently we need to use it. Consequently, this can range from 6 to 10 years. And, it all depends on how frequently the device needs to pace the heart [9].

Infusion pumps, such as enteral, Patient-Controlled Analgesia (PCA), and insulin infusion pumps can be used in a variety of treatments [10]. Infusion pumps have been linked to a number of patient safety issues. As a result, the development of authentication mechanisms is critical. In real-world applications, remote pump control is a common requirement. This is why many authors concentrate on it. For example, to avoid the implementation of encryption, the authors in [11] have developed a new protocol that can be used in the communication of remote implantable devices (such as Medtronic insulin pump), and it will rely on plain text.

A glycemia (i.e., the presence, or the level, of glucose in one's blood) alarm system is presented in [12]. This system has the ability of calculating the amount of insulin dynamically to be administered to diabetes patients. Although the wireless communication scheme may increase the security threats on these electronic devices, it remains the best desired communication scheme for the implementation of these devices. Examples of this include cable breakage and infection [13]. Figure 1 shows some of the most used IMDs and their positions in the human body.

Internet of Wearable Devices (IoWDs). Individuals wear such devices to monitor their biometrics, which may help improve their overall health. This category contains a wide range of IoMT systems. Examples of IoWDs include [14, 15]:

- EEG (electroencephalography) and ECG (electrocardiography), which are used to monitor the heart and brain respectively.
- Fall detection band, blood pressure monitors and electrocardiogram (ECG) monitors [16].
- Smart watches that are quite famous currently for monitoring biometrics like heart rate and movement. When the individual is not active, the monitoring can detect slow and fast heartbeats. The new watches can also be used for fall detection and ECG readings to detect medical conditions such as atrial fibrillation (irregular heartbeat). They are now commonly used for non-critical patient monitoring [17].
- Activity sensors which can be used to monitor actions like running and sleep.
- Accelerating sensors which are capable of tracking the patient's rehabilitation.
- Respiratory rate sensors monitoring the patient's breathing and muscle activity.
- Sensors and fitness trackers.

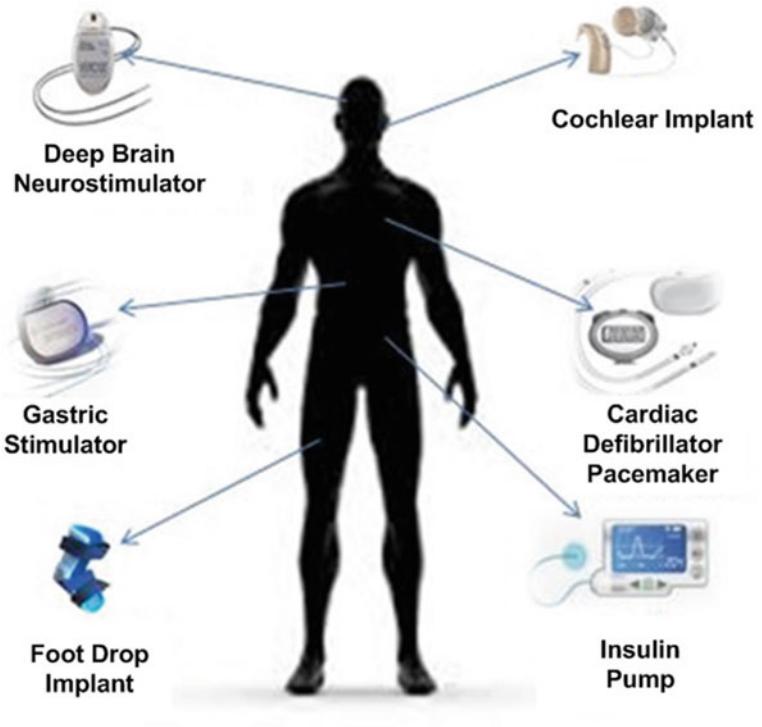


Fig. 1 Most used IMDs and their positions in the human body

However, due to battery life limitations and sensor accuracy, these devices are unlikely to be used to replace IMDs in critical situations [18].

2.3 IoMT Systems Architecture

The existing IoMT systems [19] usually have four main stages*: Sensor Layer, Gateway Layer, Cloud Layer and Visualization/Action Layer,* as shown in Fig. 2. These layers include all the steps that data passes through, from the collection of patient biometric signals via wearable sensors/devices to the final step of storage and visualization by the patient or analysis with a physician in a healthcare application.

Sensor Layer. The major function of the Sensor Layer is to establish an effective and accurate sensing technology to collect various types of health-related data [20]. The system uses implanted or worn sensors (like a pacemaker or a smart watch) to collect the patient's biometric data. These data are transmitted through wireless protocols such as WI-FI, Bluetooth or over MedRadio frequency spectrum reserved for IMDs to the second layer [21].

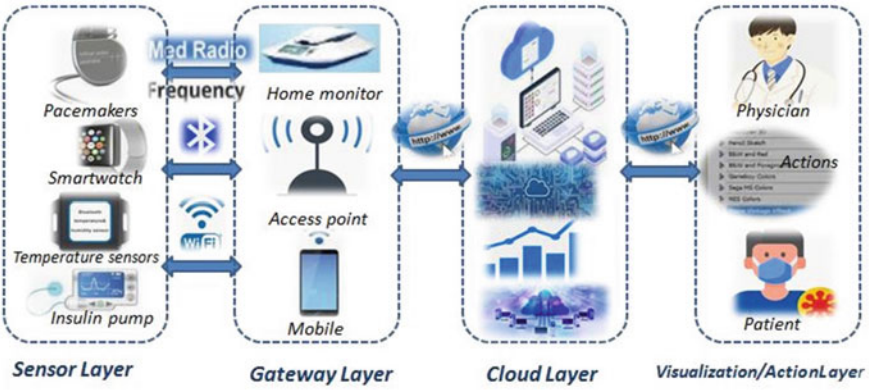


Fig. 2 IoMT system architecture

The attacks at this layer can be against the hardware or software. The system must be appropriately protected against these attacks so as to ensure the right functioning of the system and not to threaten the life of people using the IoMT.

Gateway Layer. As shown in Fig. 2, this layer acts as a bridge between IoMT sensors with low processing and storage capacity and the Cloud layer. The data is transferred to this layer without any processing. Devices that can be used in this layer include the patient's smartphone or a dedicated Access Point (AP), which can be typically more powerful than IoMT sensors. Some of their functions include performing some pre-processing operations as well as forwarding sensor data to the cloud through the Internet [22].

Cloud Layer. The retrieval and execution of the information obtained from the other layers, i.e., the sensor and gateway layer is performed at this level. Cloud servers control the systematic computing capacity. In addition to storage capacity, cloud servers also have the ability to make decisions based on the information obtained. In some critical heterogeneous IoMT applications, cloud servers can take action quickly based on emergency event detection mechanisms [23]. The analysis performed at the cloud layer includes processing data to find any changes in the patient's health. After being detected, the changes are presented to the physicians for any emergency response or patients for further actions. This layer provides a means of remote access to manage and control the various sensors.

The data in the cloud and visualization layer is mostly at rest - it is just as vulnerable as any other stage. Therefore, it is essential to protect it from unauthorized access. Attacks in this layer range from stealing account credentials to DoS/DDoS attacks [24].

Visualization/Action Layer. Data is displayed to the physician and the patient in this layer to allow for ongoing monitoring and control of the patient's condition. This layer also contains the procedures indicated by the physician in the event of a change in the patient's health; these processes can include quantity, indication, prescription or change of dosage of different medications.

2.4 IoMT Security Requirements

One of the major concerns of internet-accessible medical devices and healthcare network infrastructures is the security. In this section, we present the security requirements of future healthcare network infrastructures for IoMTs. This is based on CIANA (Confidentiality, Integrity, Availability, Non-Repudiation, and Authentication) considerations and includes the 11 security requirements listed below [22, 25, 26]:

(1) **Confidentiality/Privacy**. For the IoMT operations to be confidential, it is required to ensure that confidential information is not disclosed or made available to unauthorized parties [27, 28]. Confidentiality in the context of the IoMT refers to the protection of the medical information that the patient shares with his/her therapist, physician, or medical staff from any intrusion which can harm the patient (or a rogue entity can use the medical information against the individual) [29]. There are certainly rules for collecting and storing the patient's health data like adhering to legal and ethical privacy regulations such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act). The latter requires that only authorized individuals have access to the data. To protect the privacy of the patients' health data, adequate safeguards must be adopted so as to prevent any data breaches. Such measures should be handled seriously because cyber criminals do not only violate the patients' privacy but can also cause financial and reputational harm if they decide to sell that data in the illegal markets [29]. Fortunately, a range of approaches that can be used to ensure confidentiality are available. These approaches can make the patients' data unintelligible [28]. Currently, cryptography and access control lists are the techniques that best meet this requirement [22].

(2) **Integrity**. The data integrity requirement for IoMT health systems is to make sure that the data arriving at its intended destination has not been altered in any way during wireless transmission [30]. Integrity for IoMT data ensures that the patient's information, such as personal medical data and test results are accurate [28]. Nowadays, healthcare organizations are more aware than ever before about the importance of data integrity. The ability to detect possible unauthorized distortion or manipulation of data is critical to ensure that data has not been compromised. Therefore, appropriate data integrity mechanisms must be adopted to prevent the malicious attacks from altering transferred data. The legal and ethical GDPR state that medical providers must take the necessary steps to ensure that patient data is not altered i.e., it is accurate and up-to-date. Moreover, it insists that any altered personal data should be deleted or rectified as soon as possible [31]. The GDPR also emphasizes "*accuracy*" of data. It states that data owners should be able to request service providers to correct inaccurate information, and that service providers must respond to these requests within one calendar month. Similarly, HIPAA requires medical

providers to adopt measures to ensure that PHI (Patient Health Information) stored in systems can only be changed by legal authorization [31].

(3) **Availability**. Availability refers to the accessibility of services and data, provided by servers and medical equipment, to the affected users whenever they need them. Most importantly, these services and data will become unreachable in the event of DoS attacks. Any inaccessibility of data or services could result in life-threatening incidents for the patient, like the inability to provide early warning of a heart attack. Therefore, so as to ensure data availability to users and emergency services, any healthcare application must be *always-on*. By adopting preventive security measures and countermeasures to DoS attacks, healthcare providers can restore availability and access to personal data in a timely manner [32]. Therefore, to ensure availability, the system should be always updated to monitor any performance changes, provide suspicious data storage or transmission routes in case of DoS/DDoS attacks, and increase the performance of the systems to be able to solve any problem quickly.

(4) **Non-Repudiation**. It refers to the ability of holding any authorized user accountable for his/her actions. Simply put, non-repudiation ensures that no operation in the system can be denied [22]. This requirement prevents the authorized users from disclaiming previous commitments or actions in the system [28]. A patient might deny that some data belongs to him, when in fact the extracted data was sent from his sensors. Another case could be updating a few sensors firmware by an authorized developer, but the latter refuses to admit its validity. In many cases, if an authorized entity denies previous commitment or action, a specific procedure involving a trusted third party is usually required to resolve the situation [28]. Using digital signature techniques is the best way to meet this requirement [22].

(5) **Authentication**. This requirement refers to the ability to validate a user's identity when the user accesses the system. On the other hand, the process by which a user is verified as the original source of given data at some point in the past is known as message authentication. The most secure form of authentication is mutual authentication. In this authentication, the client and the server authenticate each other before exchanging secure key or data. Because of the lack of memory storage in several IoMT devices or insufficient CPU (Central Processing Unit) power to perform the cryptographic operations required by traditional authentication protocols, lightweight authentication protocols are becoming more popular [33].

(6) **Authorization**. It refers to confirming that authenticated users only execute commands that they are authorized to execute [34]. More specifically, authorization makes sure that only authorized entities can access to specific network services or resources, like patient's collected medical data. Permission to perform a given action, like issuing commands to medical IoMT devices or updating the medical IoMT device software is granted only for trusted expertise parties.

(7) **Anonymity**. This requirement ensures that the identity of the patient or physician remains hidden from unauthorized users when they interact with the

system, i.e., both the patient and the physician should remain anonymous. The identity of the patient/physician should not be exposed when they are in communication [35]. Passive attacks can see what you do but not who you are. This anonymity can be achieved (for instance) by using smart card like mechanisms.

(8) **Forward and Backward Secrecy**. Forward secrecy has been identified as a critical property of a variety of cryptographic primitives. It keeps the future transmitted data secure even if previous data have been compromised. However, even if the current data have been successfully attacked, backward secrecy makes sure that old data are safe. To achieve forward/backward secrecy, time-based authentication parameters must be used. The authors in [36] proposed a method that provides the secret both in front and behind the group's members. Furthermore, it provides a formal analysis of the new method's correction based on BAN (Burrows–Abadi–Needham) authentication logic.

(9) **Secure Key Exchange**. This is the requirement which means the ability to securely distribute keys among system nodes. One of the most efficient algorithms for data security is the Elliptic Curve-Diffie Hellman (ECDH) using key exchange [37].

(10) **Key Escrow resilience**. This requirement ensures that the system administrator is not allowed to impersonate any user authorized to use the system. This helps protect the system against internal threats. To meet this requirement, the Key Generation Server (KGS) only has half of the key and will be unable to compute the entire private key for both entities [38]. This requirement can be met by combining a cryptographic hash function (CHF) and asymmetric keys.

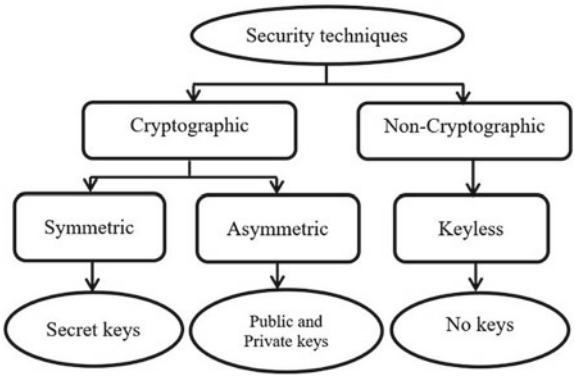
(11) **Session Key Agreement**. Following the authentication process, Session keys must be used by every node in the system. The work in [39] proposed a system in which each sensor node agrees on the generation of session keys. This scheme improves performance so that the authenticated device can calculate session key ahead of time.

2.5 IoMT Security Techniques

For securing IoMT systems, several techniques are available by this time. Based on [22] (see Fig. 3), these techniques are classified into three types (mainly): symmetric, asymmetric, and keyless. Cryptographic algorithms are used in both symmetric and asymmetric techniques, whereas keyless techniques are non-cryptographic.

(1) **Symmetric Cryptography**. Symmetrical key Cryptographic algorithms are the fundamental building blocks of any secure system that requires confidentiality. They are typically used to encrypt bulk messages transmitted between two systems. The keys used for encryption and decryption in these cryptographic algorithms are the same for both communicating entities, and this is

Fig. 3 Security techniques



shown in Fig. 4 [40]. This key must be generated and distributed prior to any communication.

In this subsection, we will look into how symmetric cryptographic algorithms can be integrated into IoMT systems.

Continuous Facial Recognition. It is the technology that allows IoMT systems to authenticate users by scanning their faces. Identity hashing and continuous facial recognition are the two steps in this technique. The ID is hashed only once, at the start of the session. After passing the identification hash test, continuous facial recognition is performed throughout the session [41]. Biometric authentication is performed in this step. Each authorized person has a set of images taken and saved with their respective roles. This technique can effectively secure the system in a medical environment due to its continuous scanning of the user's face while using the system.

Fig. 4 Symmetric cryptography operation flow

Hierarchical Access. This technique enables patients' data stored in the cloud layer to be accessed in a hierarchical manner. One approach makes use of a hierarchical role based model and gives permission based on the role of the user [26]. All authenticated nurses, for example, can dispense medications; however, in order to prescribe a new medication, a doctor is required. To support this hierarchical access, the work in [26] used the Chinese Remainder properties. It is a technique in which any patient's data can be accessed by a user with a higher privilege. The user with a lower privilege, on the other hand, can access a portion according to his role. Additionally, the work in [41] proposed a hierarchical key allocation scheme that supports dynamic updates, in particular, the concept of security against key indistinguishability. As a foundation, the authors employed a symmetric encryption scheme.

Gait-Based Technique. Gait recognition refers to the task of identifying people based on how they walk. To generate unique symmetric keys, this method employs the human walking pattern. The work in [42] demonstrates that depending on the gait, additional tasks such as gender recognition or age estimation can be processed. When more than one walk-based task is jointly trained, the identification task converges faster than when trained independently, and multi-task pattern recognition performance is equal to or better than more complex single-task pattern recognition.

CHF with XOR. Converting data of arbitrary size to data of fixed size through a one-way mathematical function is known as CHF (Cryptographic Hash Function) [43]. In order to determine whether one of its operands is different, exclusive-OR (XOR) can be used. Within the healthcare field, a sensor ID or a shared key (or any other initial parameters) can be XORed and then hashed. Then, the hashed parameters are distributed from the key generation server to the sensor and gateway nodes. These nodes are enabled by the parameters to generate keys [44]. Experimental results and theoretical analysis indicate that when combining CHF, a symmetric key, and XOR operator, the scheme significantly reduces the computational cost compared to schemes using asymmetric encryption and presents a lower security risk compared to lightweight schemes, as demonstrated in [45] and [46]. The hash function is also used in this technique to support unique identification parameters. However, initial parameters must be added manually to all nodes by the system administrators during the system's initialization step.

(2) **Asymmetric Cryptography**. Asymmetric cryptography, also known as Public Key Cryptography (PKC), refers to cryptographic algorithms that encrypt and decrypt data using a pair of related keys, the public key and the private key, to prevent unauthorized access. Everyone has access to the public key, but only the owner has access to the private key. Two popular algorithms in this technique are Rivest–Shamir–Adleman (RSA) and Elliptic-Curve Cryptography (ECC) [47, 48]. However, due to its subtle characteristics, ECC is the most widely used cryptographic technique for securing IoMT systems. A 160-bit ECC key is as good as a 1024-bit RSA key and is 15 times faster [49]. Figure 5 [40] illustrates asymmetric encryption which uses two keys, mathematically linked but distinct to encrypt (public key) and decrypt data (private key).

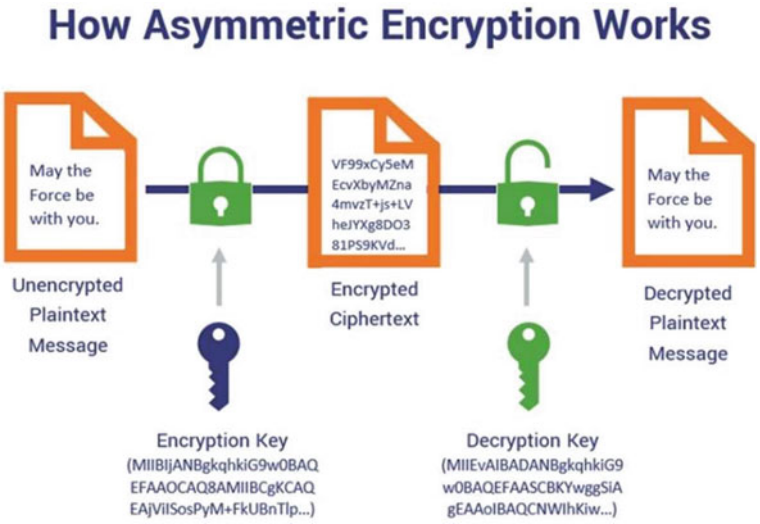


Fig. 5 Asymmetric cryptography operation flow

CHF with ECC. When used in conjunction with ECC keys, the CHF feature allows the establishment of a secure, *certificateless* channel between patients and their physicians [25]. The two techniques are combined to provide a secure method for sharing keys between different layers of IoMT. After the nodes receive the hashed values, they can be used to generate their asymmetric keys. This technique can also reduce the overhead associated with certificate management for cloud data storage and sharing [50].

Homomorphic Encryption (HE). Homomorphic encryption allows for the secure transmission and storage of confidential information across and within a computer system [51]. HE attempts to help in the encryption process by allowing certain types of computations to be performed on ciphertext. This process ends up with an encrypted result that is also in ciphertext. Its output is the result of operations on the plaintext. However, this technique is different from others because it does not allow the medical staff to see the patient data. Only the patients can have access to their data, except in emergencies. This is helpful for some IoMT sensors, like smartwatches.

There are three types of HE schemes: partial HE (PHE), which can perform a single mathematical operation an infinite number of times; somewhat HE (SHE), which can only perform a limited number of operations; and fully HE (FHE), which supports an infinite number of operations. Thus, among the three schemes, the FHE is the most suitable for fast data aggregation without compromising data confidentiality [49]. Optimal HE (OHE) is an FHE variant that is best suited for hospital healthcare monitoring systems. The key is authenticated during encryption, and the best key is chosen using the Step Size Fire Fly (SFF) optimization algorithm. This strategy can

be used to generate the encrypted key while achieving maximum key breaking time and minimal computational time while maintaining high security [52].

Digital Signatures. These techniques are frequently used to validate the authenticity of data/commands by signing and verifying them with the sender's private and public keys, respectively [53]. Digital signatures can be embedded into sensor firmware in IoMT systems using an add-on software shim, allowing it to validate and intercept sensor wireless communications [54]. The sensor's firmware must store a list of authorized users' public keys in order to validate these techniques. The work in [55] propose a scheme for authenticating a device that includes multi-factor authentication, digital signatures, and device capability. The proposed scheme not only efficiently authenticates the device via multi-factor authentication, but also it authenticates the authentication server via digital signatures.

Smart Cards. Smart cards in healthcare systems are thought to have enormous potential for improving healthcare delivery as well as lowering healthcare costs. Because of its reliance on physical keys, this technique is different from the previous techniques [56]. With ECC keys serving as the first factors, the physical keys serve as the second for authentication. To gain access to a system IoMT, the user must first enter an access key before using their smart card. Apparently, this technique helps the system resist cyber break-ins if one of the two factors is compromised. This is why smart cards are quite common these days.

(3) **Keyless Techniques**. In this subsection, we explain the keyless techniques that provide security without using pre-shared keys.

Biometric Technique. Owing to its simplicity, this technique has become the most used technique to ensure IoMT systems. This technique uses biometric sensors to identify users' physical characteristics such as, fingerprint sensors, which can read the fingerprint image, and ECG-based sensors that record heartbeat activities in order to encrypt data. There are different fingerprint authentication algorithms such as: Delaunay triangulations, polar coordinates and Minutia Cylinder-Code (MCC) [57]. The performance and complexity of the applied algorithm determines the performance of the device used. The Finger to Heart (F2H) IMD fingerprint authentication algorithm based on Minutia Cylinder-Code (MCC) is proposed to ensure the safety of IMDs such as pacemakers and defibrillators. This improved algorithm significantly reduces both message size in transmission and device computational overhead, while conserving IMD's limited resources [58].

Token-Based Security. The use of passwords or predefined keys presents many problems that limit their applicability for various IoMT applications. Whether software or hardware, tokens can be used for user authentication. The use of lightweight token-based user authentication (TBL UA) for IoMT devices, based on the token technique, improves the robustness of authentication [59]. Radio Frequency Identification (RFID) can also be used as a hardware token in a hospital information system (HIS) for secure sensor logistic management [60]. The work in [61] proposes an implementation of MQTT (Message Queue Telemetry Transport) protocol token authentication in constrained devices. According to the results of the usability and

performance tests, the system can perform valid and expired token authentication in a reasonable amount of time.

Blockchain Technology and AI. Due to their impact with their advanced distributed security and remarkable role in securing other fields like finance, Blockchain and Artificial Intelligence (AI) have become the key technology for the requirements of IoMT systems, mainly to bring transaction and data processing at the cloud layer [62]. In IoMT systems, the blockchain technology is used as a security management to share information between the patient and other parties like the doctors. AI systems, on the other hand, can detect intrusions or anomalous behavior in patient data and network flows. Nevertheless, these techniques still face some challenges that allow them to be implemented in the IoMT systems that are discussed in [63, 64].

3 Risks and Attacks in IoMT

In this section, we will discuss the possible physical and network attacks that threaten the IoMT systems and how to avoid or mitigate them.

3.1 Physical Attacks

In this type of attack, the attacker must be physically close to the network or devices of the system in order to launch the attack wirelessly [65]. To extract security keys or patient data, the attacker targets the physical components of the IoMT systems. Some of the common types of physical attacks are the following:

Physical Security Token Loss. It is when the attacker steals a physical security token, like a smart card or proximity card, from an authorized user in order to have access to the system. The security requirements violated in this case are authentication, authorization, anonymity, and forward secrecy. As the smart card or proximity card alone is insufficient to hijack the system, authentication based on ECC combined with smart cards can be used to protect the system against this type of attack [56].

Impersonation attacks. The attacker pretends to be a legitimate entity or an authorized user to access resources to which he is not authorized. Bluetooth Impersonation Attacks (BIAs) are effective against any Bluetooth device, and they are undetectable because the Bluetooth standard does not require notifying end users of the outcome of an authentication procedure or the lack of mutual authentication [66]. To avoid such attacks, cryptographic techniques such as, CHF and biometrics should be employed.

Tampering. It is an attack in which the attacker physically modifies the data of the IoMT systems [67]. Any modification in a device like RFID or communication link is considered a tampering attack. Altering the IoMT data by attaching external devices and attacking sensors is also considered a tampering in an emergency. However, this

attack can be mitigated if symmetric keys are combined with facial recognition or if keyless methods are employed [41, 57].

Side Channel. These attacks rely on information achieved from the encryption device's side channels. In addition to plaintext and ciphertext messages, they are used to recover the secret key using electromagnetic analysis, power consumption or, differential power consumption during encryption/decryption of various messages and during computation of various security protocols [68]. In addition to cryptography techniques, the Datagram Transport Layer Security (DTLS) protocol can be used to avoid such attacks as the work presented in [69] recommended. On the other hand, Blockchain technology and AI were demonstrated as additional detection and mitigation strategies in [62].

Radio Frequency (RF) Jamming/Desynchronization. This is another serious type of attack on the IoMT systems. Because IoMT sensors are limited in energy by the battery, they may cause battery discharge. Blockchain and AI technologies have the potential to mitigate the effects of these intrusions by finding alternate routes or cutting off the canal's connection to the attacker [70].

Fake Node Injection. In this intrusion technique, to control data flow between two legitimate nodes of the network, the attacker drops a fake node between them [65].

Permanent Denial of Service (PDoS). Also known as Phlashing, PDoS is a type of DoS attack in which hardware sabotage completely destroys an IoMT device. The attacker launches the attack using a malware to destroy firmware or to upload corrupted BIOS (Basic Input Output System) [45].

Sleep Denial Attack. In this attack, the battery powered devices are kept awake by the attacker who feeds them with wrong inputs. The batteries eventually get exhausted and thus cause the devices to shutdown [65].

Malicious Code Injection. In this intrusion technique, a malicious code is injected onto a physical device by the attacker. By compromising this device, the attacker may be able to launch other attacks as well [65].

The physical attacks, their effects, and the solutions proposed are summarized in Table1.

3.2 Network Attacks

Bluetooth and Internet connections (wireless) can be targets of various types of attacks at different layers of the IoMT system. Stealing or fabricating patients' data, creating congestion, jamming, or connection blocking can affect normal operations or result in a total communication failure, which is usually the primary objective of these kinds of attacks.

Man-In-The-Middle (MITM). It is an attack that targets the communication between two IoMT devices and gives access to their private data. In this attack, the attacker is able to eavesdrop or monitor the communication between the two devices [67]. The intercepted data can be modified by the attacker before it is sent to

Table 1 List of physical attacks, effects and proposed solutions

Physical attack	Effects	Proposed solution	Solution references
Physical security token loss	Authentication; Authorization; Anonymity; Forward secrecy	Asymmetric (two-factor)	[69, 71]
Impersonation/Presentation		Asymmetric; Keyless	[25, 57, 58, 69],
Tampering/Malicious code injection	Data confidentiality; Data Integrity	PUF (Physically Unclonable Function) based Authentication; Symmetric (two-factor); Keyless	[41, 50, 57, 69] [57]
Side channel attack	Collect Encryption Keys; Data confidentiality; Data Integrity	Masking technique; Authentication using Physically Unclonable Function (PUF); Keyless	[50, 62, 69, 72]
Radio frequency (RF) jamming/Desynchronization	Battery discharge; Availability	CUTE Mote; Keyless	[70, 73]
Permanent denial of service (PDoS)	Hardware sabotage completely destroyed	NetwOrked Smart object (NOS) Middleware	[74]
Fake node injection	Control data flow and drops a fake node	Pervasive Authentication Protocol (PAuthKey)	[75]
Sleep denial	Node put on awake or shutdown	CUTE Mote; Support Vector Machine (SVM)	[73, 76]

its original destination. For instance, a patient biometric data, which is transmitted between any two layers of the IoMT system, may be altered or modified. As explained in [77], this is possible with the use of Unmanned Aerial Vehicles (UAVs) that result in a Drone-in-the-Middle (DitM) attack. MITM can be made even more powerful if the UAV is linked to a cloud, allowing it to perform more intensive computation in a relatively shorter amount of time.

DoS/Distributed DoS (DDoS). Unlike DoS attacks, which were perpetrated by a single node, a DDoS attack involves multiple sources attacking a specific target by flooding it with messages or connection requests with the goal of making service unavailable, preventing legitimate users of a service (i.e., from using it) [78]. Network fragmentation can also occur because of such attacks. Typically, the cloud layer is the main target for these attacks so as to make the system unavailable to users [79].

Consequently, availability is the violated requirement in this type of attacks. Similar to Radio Frequency (RF) Jamming attacks, Blockchain technology and AI can find alternative paths or terminate the connection to the channel controlled by the attacker, and thus can mitigate these attacks [70].

Clock Synchronization. IoMT systems, like all real-time systems, require a clock synchronization protocol. The latter is the target of this type of attack. The secure key exchange is the violated requirement in this attack. This attack is considered serious because the attacker can make other attacks (such as relay, replay, and MITM) difficult to detect [22]. However, the combination of ECC with smart cards can be used to mitigate this kind of intrusion [56].

Sniffing. Sniffing attacks passively intercept data sent between two nodes. This attack results in a breach of patient data confidentiality as the attacker can see the data transmitted between the system's layers [77]. Thus, the data confidentiality is the violated requirement in this attack. To mitigate this type of attack, any encryption algorithm, whether symmetric, asymmetric, or keyless can be used.

Relay. The intercepted data, after a successful sniffing attack, can be relayed to a third node without modifying it by the attacker. For instance, the intercepted patient data can be redirected to the attacker's device before being sent to its final destination [70]. The authorization requirement is violated by this attack. Techniques such as hierarchical access and secure session keys can be used to mitigate this.

Replay. In this case, a signed packet may be captured by the attacker who would resend the packet several times to the destination [52]. As a result, a DoS/DDoS attack is possible. The authorization requirement is violated with this attack. To mitigate these attacks, a *timestamp*, which is part of some cryptography techniques, can be used [62].

Brute Force. Typically, in this type of intrusion, the attackers use automated software that generates different password combinations until it succeeds. The strength of these attacks stems from the fact that the passwords chosen by the user are inherently weak, or it employs default generated passwords or username as password [42]. An example, which is a significant problem for IoMT devices, is the dictionary attack. The latter relies on passwords or known words in dictionaries. After capturing the encrypted/decrypted data with machines or more powerful tools, these attacks can also be carried out offline. A dictionary attack is considered a dangerous attack for IoMTs, because the password selection criteria can be guessed with a simple python script [80]. Security requirements for authentication and authorization are violated through such attacks; however; they can be mitigated with the use of keyless methods like biometrics.

Selective Forwarding. In this attack, some messages may be simply altered, dropped, or selectively forwarded to other nodes in the network by a malicious node [52]. As a result, the destination receives incomplete information.

RFID Spoofing. To gain access to the information printed on the RFID tag, the attacker first forges an RFID signal [65]. Then, he/she can send his/her data as valid using the original tag identifier [81].

RFID Unauthorized Access. An attacker can update (i.e. read, modify, or delete) data on RFID nodes because of the lack of proper authentication mechanisms, [82].

Table 2 List of network attacks, effects and proposed solutions

Network attack	Effects	Proposed solution	Solution references
MITM	Data confidentiality; Authorization	Symmetric/Asymmetric (two-factor); Keyless	[25, 71]
DoS/DDoS	Availability	Keyless	[70]
Sniffing	Data confidentiality	Symmetric/Asymmetric (two-factor); Keyless	[62, 77]
Relay	Authorization		[70, 71]
Replay			[41, 46, 56, 62]
Clock synchronization	Secure Key; Exchange	Asymmetric (two-factor)	[56]
Brute force	Authentication; Authorization	Keyless	[42]
Selective Forwarding	Data confidentiality; Data Integrity; Authentication; Authorization	Hash Chain Authentication technique with Rank Threshold; Monitor based approach (CMD)	[71, 83]
RFID spoofing/RFID unauthorized access		SRAM based PUF	[84]

Table 2 summarizes the network attacks, their effects and the corresponding solutions proposed.

4 Security in IoMT Communication Protocols

In this section, we explore the communication protocols of IoMT. According to [85], the IoMT system can be divided into three main layers: the perception, network, and application layers. There are two more sub-layers between these three main layers: the adaptation layer, which includes the protocols that communicate between the perception layer and the network layer [86], and the transport layer, which also includes the protocols that transport information between the network and application layers [87]. We also present for each layer the most documented security measures, mitigation and implementation for each protocol to secure modern healthcare infrastructures and networks.

Figure 6 shows the different layers of IoMT systems in relation to the OSI (Open Systems Interconnection) reference model. This classification is based on the protocols and functions that each layer requires. The perception layer is primarily used for hardware functions. The network layer is responsible for network functions, while the application layer is designated for user functions.

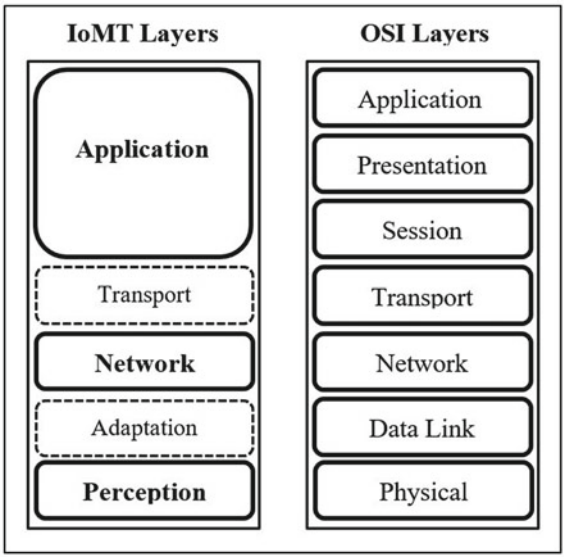


Fig. 6 IoMT versus OSI layers

4.1 Perception Layer

The majority of the perception layer protocols are based on or implement the IEEE 802.15.4 standard [88, 89]. To collect information about the patient's health status from sensors, health systems have used the following perception layer protocols and mechanisms:

RFID. Radio Frequency Identification (RFID) is a wireless object identification technology which uses radio frequency signals for very short range communications [90]. Autonomous RFID tag technology that is placed in or near the patient's body plays an essential role in the development of body health systems [91]. Moreover, passive RFID tags can be used in several situations such as; patient environment monitoring, physical access control [90, 91], and storage temperature monitoring for each type of drug [92, 93].

RFID is a technology that is used in devices with very low-power features, making common security mechanisms difficult to implement. However, researchers have proposed several noteworthy custom authentication mechanisms. An RFID tag authentication protocol is proposed in [94] that requires less storage and computation on the tag side. This protocol protects against replay, DoS, forward and backward tracing, and server impersonation, as well as provides privacy and security features. On the other hand, a hash-based RFID security protocol with forward privacy is presented in [95]. Its main aim is to protect the RF tag from tracking attacks by observing previous unsuccessful tag sessions. Furthermore, partial solutions to various limitations are identified and proposed in [96]. Examples include: dynamic password, synchronized secrets and custom system authentication systems.

NFC. NFC, or Near Field Communication, is a protocol that is used to connect IoT devices in a simple and low-cost manner [93, 97]. However, when NFC is used in IoT devices in the medical field, a number of biocompatibility issues arise. This infrastructure has the potential to provide convenient and low-cost power distribution and communication channels for a variety of medical devices. In addition, a battery or external electrical connection is not necessarily required in NFC-enabled medical devices for their custom operations [98]. An NFC device embedded in a cell phone, for example, can transmit pacemaker measurements to a monitoring doctor, control an insulin pump remotely, or activate an implanted neural simulator [92].

NFC implementations can be theoretically attacked by MITM attacks; however, it is extremely complicated to launch these attacks in real-world executions because of the NFC's architecture and distance limitations [99] (even if tried wirelessly). Moreover, a list of known security issues with the NFC protocol is presented in the existing literature like for instance, in [100], where some practical countermeasures are also suggested for each of the attacks mentioned. Furthermore, a single and multiple antenna design for the NFC controller component is suggested in [101], in order to mitigate attacks like, data corruption, low battery, and tag cloning.

Bluetooth/BLE. Bluetooth is a wireless technology that is based on the IEEE 802.15.1 standard. It is a low-power, low-cost wireless communication technology that can transmit data between mobile devices over a short distance (8–10 m with 2.4 GHz band). Bluetooth Low Energy is the ultra-low power, low-cost version of this standard (BLE or Bluetooth Smart) [90]. In addition, these features make Bluetooth/BLE more suitable for IoMT devices such as IoWDs and human interface (HID) devices [102].

Different attacks may threaten devices which are connected through BLE, and according to published research works, these threats are across all communication layers. Nevertheless, a variety of security controls to mitigate such attacks are provided by BLE implementation [103]. To achieve confidentiality and integrity, some solutions employ AES-CCM encryption. To authenticate data channel packet data units (PDUs), a 4-byte MIC module can also be used [104]. Furthermore, in order to protect Bluetooth Low Energy (BLE) technology from attacks, the authors in [105] propose a set of techniques and countermeasures that can be used to secure Bluetooth communications.

Z-Wave. Z-wave is a low-power wireless MAC protocol developed by Zensys. It is used for remote control applications and small commercial domains [90]. This protocol supports two types of devices: control devices and slave devices [106]. Z-wave can also support short messaging between IoMT devices for light, energy, and healthcare control [87].

Z-Wave provides confidentiality, source integrity, and data integrity services through AES (mostly 128) encryption, policy-driven and behavior detection mechanisms. The security command class included in the Z-wave allows application frames to be encapsulated in an encrypted and signed security frame. Symmetric encryption protects the frame by using AES with three shared keys known by every network node that needs the security service [107]. Furthermore, techniques like hiding the WLAN SSID (Service Set IDentifier), using WPA2 (Wireless Protected Access 2) instead of

WEP (Wired Equivalent Privacy), and Reverse Proxy Server can also provide extra protection for IoMT devices using Z-wave [108].

UWB. UWB (Ultra-wideband) technology is based on the IEEE 802.15.3 standard, which has recently gained popularity as a method of high-speed, short-distance indoor wireless communication [109]. One of the most intriguing aspects of UWB is its bandwidth of more than 110 Mbps, which is sufficient for most multimedia applications and is applicable for hospitals. UWB for medical systems is suggested in [110] because when communicating with implanted sensors, high signal attenuation requires a protocol that transcends channel limitations. It works by transmitting signals from sensors to a microcontroller [93]. For instance, a short distance communication technology is required by the electrocardiogram procedure and this is the aim of using UWB (among other protocols) [97, 111, 112].

Being a distance protocol, UWB is threatened by attacks that differentiate the distances between nodes. UWB adopts the Advanced Encryption Standard (AES) block cipher with counter mode (CTR) and cipher block chaining message authentication code (CBC-MAC) [113]. In [114], a Verifiable Multilateration (VM) algorithm that uses verification triangles to detect a distance enlargement attack is suggested. A location-based secure authentication scheme is proposed by other works like [115, 116] to prevent external attacks. In addition, [117] suggests the first modulation technique to prevent ED/LC (Early Detect/Late Commit) attacks regardless of communication range in the UWB with pulse reordering (UWB-PR).

Table 3 summarizes these issues discussed so far.

4.2 Network Layer

The network layer is responsible for the transmission and reception of the collected medical data. As a result, this layer serves as the foundational infrastructure layer for the healthcare platform. As such network devices transfer sensitive data, network security is a major concern in the field of healthcare [131]. The IEEE 802.15 standard is the foundation for the majority of the protocols in this layer [132]. The following protocols are the most commonly used for IoMT at this layer:

WiFi. Wireless Fidelity (Wi-Fi) is a middle-range (up to 100 m) protocol based on the IEEE 802.11 family of standards [133, 134]. A number of authors have proposed using Wi-Fi to communicate with monitoring devices in an IoMT system. For instance, the authors in [135] use this protocol on a network of 45 critical medical care devices, demonstrating that communication between these devices is effective and secure via Wi-Fi. Moreover, this protocol is used in a system for remote patient health monitoring in conjunction with Global System for Mobile communication (GSM) to simulate the transfer of medical data between two different geographical locations [136].

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the mechanisms used to secure Wi-Fi 802.11

× communications. WPA technology is characterized by providing more powerful encryption mechanisms [137].

ZigBee. ZigBee is a wireless communication protocol that conforms to the IEEE 802.15.4 standard and is intended for low-power, low-cost, low-speed wireless personal area networks that connect devices primarily for personal use [138]. This protocol is used by health zones to connect sensors to the coordinator, as well as

Table 3 Perception Layer protocols—security level, attacks and countermeasures

Protocol	Security level	Attacks	Countermeasures proposed	References
RFID	Several weaknesses in the active and passive RFID systems; Requires the integration of special security mechanisms into the system to ensure the fundamental security requirements	Side channel attacks backward/forward traceability	Encrypted RFID implementations; hash-based RFID security protocol;	[118–120]
NFC	Data exchange in close proximity; Several threats in transactions or contact processes (requires data encryption before any communication or transaction)	Eavesdropping; MITM; Data Modification; Data Insertion and Data Corruption attacks	Communication distance limitation; integrate standard cryptographic practices to protect its communication channel and data	[121, 122]
Bluetooth/BLE	The link keys may be stored incorrectly; The length of the encryption keys may be small or only 1 byte; No user authentication	Sniffing, DoS, MITM, PIN Cracking Attacks and Brute-Force Attacks	AES-CCM; AES-128 bits; Use link encryption and combination keys	[123, 124], [125, 126]
Z-Wave	Not enforcing a standard key exchange protocol; The source and destination fields of the MPDU (MAC protocol data unit) aggregation frame are implicitly trusted by Z-Wave devices	Key Reset, Black Hole, impersonation and node spoofing attacks	AES-128 encryption using three shared keys	[127]

(continued)

Table 3 (continued)

Protocol	Security level	Attacks	Countermeasures proposed	References
UWB	Incorrect access control configuration, Symbols with a long size	Same-Nonce, ED/LC attacks	AES block cipher with counter mode (CTR) and cipher block chaining message authentication code (CBC-MAC); The distance between nodes is secured by location and distancing protocols	[128–130]

between the coordinators themselves [139]. Implementing a fully working application layer protocol for healthcare environments, the ZigBee Health Care Profile is based on ZigBee Pro [140]. To enforce MAC layer security, ZigBee uses The IEEE 802.15.4 standard to employ higher layers. AES is used for symmetric key cryptography in implemented security mechanisms. Several other security modes are defined in [141, 142]. The authors in [143] propose a framework capable of predicting and protecting against various potential malicious attacks in the ZigBee network and responding appropriately by notifying the system administrator. It can also make instantaneous automated decisions based on real-time data defined by the system administrator.

WIA-PA. WIA-PA is a Chinese industrial wireless communication standard for process automation [144]. Despite being an industrial protocol, the work in [145] proposes WIA-PA as a transmission protocol in the internal networks of wireless sensor network, in medical remote monitoring system. The WIA-PA network's MAC layer security is based on IEEE STD 802.15.4–2006. Above the MAC layer, it provides two levels of security services: end-to-end security in the application sub layer and point-to-point security in the data link sub layer (DLSL). Furthermore, WIA-PA provides a secure access authentication mechanism for the entire network [146]. WIA-PA architecture was proposed by Wang et al. for device authentication [147]. Access is authorized through WIA-PA by using a join key shared by a device and a security manager. A security mechanism for WIA-PA and its protocol stack is also suggested and implemented in [148].

6LoWPAN. 6LoWPAN is an IPv6 adaptation layer that defines mechanisms for enabling IP connectivity for tightly resource constrained devices communicating over low power, lossy links such as IEEE 802.15.4 [93]. In the healthcare sector, IoMT sensors and local devices can be linked to IP networks via 6LoWPAN [149]. Moreover, the interconnection of sensors with middleware devices or Internet-connected routers is allowed by 6LowPAN [150]. Security protocols for different layers of the 6LoWPAN stack have been developed. The MAC security sub layer of IEEE

802.15.4 provides hop-to-hop security for the wireless medium, while the upper layer security is defined to provide end-to-end security between two remote peers [151]. The 6LowPAN security measures are classified into two taxonomies in [152]. The first is about communication outside of the 6LowPAN network (use DTLS (Datagram Transport Layer Security), HIP (Host Identity protocol) and IKE (Internet Key Exchange) technology). The second is about "*protocols inside communication*" (use IDS tool).

LoRaWAN. Originally developed by Semtech, LoRa (Long Range) is a physical layer protocol made to support low-power and wide area networks [153]. LoRaWAN, on the other hand, defines the network's communication protocol as well as the underlying system architecture [154]. An loT-based health monitoring system is presented in [155]. In this system, the medical data collected by sensors is sent to an analysis module via secure, low-cost and low-power communication links, provided by an infrastructure LoRaWAN network. Moreover, an IoMT biofluid analyzer which uses LoRa and Bluetooth is presented in [156] in order to support long-range data transmission.

LoRaWAN uses the 128-bit Advanced Encryption Standard (AES128) to ensure complete network security, including mutual end-point authentication, data origin authentication, replay and integrity protection, and privacy. A 128-bit AES key (called AppKey) and a globally unique identifier based on EUI-64 are used to uniquely identify each LoRaWAN device [157, 158].

Table 4 summarizes the Network Layer protocols' security level, attacks and countermeasures proposed.

4.3 Application Layer

The application layer is responsible for managing the smart medical platform, which includes custom interfaces and role-based control panels for diagnostic decision making. The most commonly used IoMT protocols in the application layer are listed below:

HL7. HL7 is a set of standards that enable the exchange, integration, sharing, and retrieval of electronic health information between various health entities, allowing for the development of flexible and effective processes [167]. For its great importance, it is recognized as the most widely used application layer protocol in the healthcare systems [168]. The transparency of the information flow between health care systems is ensured by this protocol. In addition to clinical practice, HL7 supports the delivery, management and evaluation of health services [169].

Protecting data is the major aim from the security scope, because HL7 transmits data that may have a high impact. Many institutions rely on SSL VPNs (Secure Sockets Layer Virtual Private Networks) and similar solutions to protect the entire network. Deidentification/anonymization is helpful in protecting patient data [170].

CoAP. The Constrained Application Protocol (CoAP) protocol was originally designed for web transfer in the IoT with limited nodes and networks. The initial

Table 4 Network Layer protocols' security level, attacks and countermeasures

Protocol	Security level	Attacks	Countermeasures proposed	References
Wi-Fi	The devices' lack of granular authentication; Weakness and limited protection against DoS attacks and service integrity	Replay, Channel, DoS, Sniffing, MAC Spoofing, and packet analysis attacks	WPA and WPA2 security technology, 128-bits WEP authentication	[137]
ZigBee	Using unsecured key transport for pre-shared keys; PAN IDs do not have verification; There are no integrity checks in ACKs, and network keys are not properly registered	Key Sniffing, Association Flooding, Device Spoofing, DoS, jamming, Replay and Energy-consuming attacks	Symmetric cryptography, AES-CTR, AES-CCM, AES-CBC-MAC, 128-bit AES-based encryption system	[159–161]
WIA-PA	There is no public key or encryption algorithm, no intrusion prevention, and the first request is not encrypted	selective forwarding, Interference, Jamming, tampering, Traffic analysis attacks	Adaptive frequency switch (AFS), Adaptive Frequency Hopping (AFH), Timeslot hopping (TH) and message integrity (MIC)	[162]
6LoWPAN	The IP network and the radio signal are the targets of 6LowPAN attacks, Vulnerabilities at its fragmentation mechanism, Node's IP address remains unchanged	Signal jamming, Replay, Flooding and Traffic analysis attackers	DTLS cryptographic techniques; Internet Key Exchange technology (IKE); HIP host identification technology	[163–165]
LoRaWAN	Using a post-message dictionary, Resetting frame counters without recoding, Caching and replaying ACK packets, and Waking up sensors using forged gateway beacon transmissions	Replay, Plain text recovery, Denial of packet delivery, The battery exhaustion, Selective DoS and MITM attacks	AES -CMAC, MIC, AAES-CTR	[166]

motivation for developing this protocol was to meet the high requirements of the IoT as well as the need for a lightweight, low-rate protocol. This protocol is specifically suited to IoMT constrained nodes with limited memory and processing power [171]. CoAP, along with the MQTT protocol, is used in a proposed system in [172] for securing real-time health monitoring systems, to protect sensor data from security breaches during its continuous transmission over the layers. To avoid breaches such as data theft and DoS attacks, strong authentication techniques should be used. It is recommended to use an intrusion detection system to detect any malicious activity in the system [173]. DTLS can also be used to protect data [174].

MQTT. Message Queue Telemetry Transport (MQTT) is a standardized publish/subscribe Push protocol developed by IBM in 1999. This protocol is used by IoMT developers due to its low memory consumption and low bandwidth requirements; MQTT was designed to send data accurately even with long network delays and limited bandwidth [171]. A Blockchain-based medical application that connects various devices to an IoMT platform via MQTT is created in the work presented in [175]. In addition, the work in [136] proposed a system to connect a remote healthcare unit as it is inside the hospital, which uses the MQTT protocol to transfer measured data from the healthcare unit to the hospital's gateway.

Unfortunately, the MQTT protocol only supports authentication for the security mechanism, which does not encrypt data in transit by default. As a result, implementing this protocol raises concerns about confidentiality, authentication, and data integrity. MQTT brokers may require username/password authentication to ensure security, which is handled by the TLS/SSL (Secure Sockets Layer/Secure Socket Layer) protocol [176].

HTTP. There are different uses of this protocol in the IoMT. For example, it is used in a system that also includes a portable medical module with a pulse oximeter and an accelerometer that communicates with the microcontroller via a custom display to which a ZigBee module is connected. The goal of this system is to track the speed and direction of movement as well as the pulse and oxygen saturation of the blood [177]. Furthermore, it is used by the work presented in [12] to provide a system capable of dynamically assessing the amount of insulin needed to be administered to diabetic patients.

In order to make this protocol more secure, it is implemented on top of an encryption layer like SSL or TLS, to form its secure version https; with an '*s*' at the end to indicate that the data is exchanged securely via an encrypted tunnel using the SSL or TLS protocol. HTTPS client authentication is done below the protocol level (at the transport level). Only the server side of an SSL connection must use a certified public key from a server certification. This method is appropriate when the client wants to ensure that it is communicating with the intended server, but if the server needs to authenticate the client, it can use a traditional authentication mechanism (basic HTTP authentication or form authentication). On the other hand, Mutual SSL authentication, also known as two-way SSL authentication, necessitates the use of certified public keys by both the server and the client of the SSL connection. The server identifies the client in this case based on the client certificate used to establish the SSL connection [178].

Table 5 Application Layer protocols' security level, attacks and countermeasures proposed

Protocol	Security level	Attacks	Countermeasures proposed	References
HL7	No security integration; the size of HL7 and sources of messages are not validated by default	Spoofing attacks; DoS and flooding attacks	SSL VPNs; Deidentification/anonymization	[170]
CoAP	Type of DTLS implementation at the proxies level (multicast or unicast)	Parsing attacks; Caching attacks Amplification attacks; Cross-Protocol and Spoofing attacks	DTLS; TLS; CoAPs	[180, 181]
MQTT	No specific security mechanism	Eavesdropping; DoS; Timing attacks; Access, modify or redirect accessible data to an untrusted server	SSL/TLS	[182, 183]
HTTP	Insecure by default; Default HTTP implementations are not encrypted	Eavesdropping; injection and manipulation attacks	SSL/TLS (HTTPS version)	[184]

Tables 5 summarizes the Application Layer protocols' security level, attacks and countermeasures proposed.

5 Conclusions and Future Research Directions

The use of IoMT has recently grown in popularity. The majority of current studies are concerned about how medical and health-monitoring devices can help reduce healthcare spending and improve patient health. As a result, securing this technology has become extremely important since this IoMT is vulnerable to different attacks mainly because of its heavy reliance on wireless connectivity. These attacks can breach the system and invade the privacy of patients and affect the medical services' confidentiality, integrity and availability. Throughout this chapter, we have shown and explained the major security problems, challenges and drawbacks facing IoMT. In addition, we have discussed the way to secure the IoMT domains and their associated assets through varied suitable security measures to enhance IoMT services as well

as the way to better the patients' health and experience via different techniques. Moreover, we have highlighted the importance of an effective security policy of different wireless communication protocols used by the IoMT system in order to keep it secured, private, trusted, and accurate.

In short, the purpose of this chapter is to highlight the relations between various technical and non-technical solutions to guarantee a secure and efficient system in all IoMT domains. Therefore, the chapter in hand gives some open research areas on security issues in IoMT both for traditional and novel-technology based solutions. To conclude, the need for developing robust security solutions using the latest technologies like Artificial Intelligence, Big Data and Blockchain is significantly growing as the IoMT are nowadays widely applicable.

References

1. I. T. Dunlap, The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History, https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/. Accessed: 30 Jan. 2022
2. A.J. Bamidele, R. Ogundokun, S. Misra, Cloud and IoMT-Based Big Data Analytics System During COVID-19 Pandemic, in *Efficient Data Handling for Massive Internet of Medical Things* (Springer, 2021), pp. 181–201
3. A-S.K. Pathan, Z.M. Fadlullah, S. Choudhury, M. Guerroumi, Internet of Things for smart living, Spec. Issue Wirel. Netw. Springer, 2019 **27**, 4293–4295 (2021), https://doi.org/10.1007/s11276-019-01970-3
4. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
5. R.A. Khan, A.-S.K. Pathan, The state of the art Wireless body area sensor networks—a survey. Int. J. Distrib. Sens. Netw., SAGE publications **14**(4) (2018). https://doi.org/10.1177/1550147718768994.
6. S.S. Ahamad, A.-S.K. Pathan, A formally verified authentication protocol in secure framework for mobile healthcare during COVID-19-like pandemic. Connect. Sci., Taylor & Francis **33**(3) (2021). https://doi.org/10.1080/09540091.2020.1854180.
7. M. Haghi, K. Thurow, Habil, R. Stoll, M. Habil, Wearable devices in medical internet of things: scientific research and commercially available devices. Healthc. Inf. Res. **23**(1), 4–15 (2017)
8. R. Altawy, A.M. Youssef, Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices. IEEE Access **4**, 959–979 (2016). https://doi.org/10.1109/ACCESS.2016.2521727
9. Pacemaker, Mayo Clinic, https://www.mayoclinic.org/testsprocedures/pacemaker/about/pac-20384689. Accessed 25 Dec. 2021
10. B.R. Larson, Y. Zhang, S.C. Barrett, J. Hatcliff, P.L. Jones, Enabling safe interoperation by medical device virtual integration. IEEE Design & Test **32**(5), 74–88 (2015). https://doi.org/10.1109/MDAT.2015.2464813
11. T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, M. Guizani, New plain-text authentication secure scheme for implantable medical devices with remote control, in *Proceedings of the GLOBECOM 2017 IEEE Global Communications Conference*, Singapore, 4–8 December 2017, pp. 1–5, https://doi.org/10.1109/GLOCOM.2017.8255015.
12. S. Sicari, A. Rizzardi, A. Coen-Porisini, How to evaluate an Internet of Things system: models, case studies, and real developments. Softw. Pract. Exp. **49**(11), 1663–1685 (2019)

13. J.E. Ferguson, A.D. Redish, Wireless communication with implanted medical devices using the conductive properties of the body. Expert Rev. Med. Devices **8**(4), 427–433 (2011). https://doi.org/10.1586/erd.11.16
14. N. Scarpato, A. Pieroni, L. Di Nunzio, F. Fallucchi, E-health-IoT universe: a review. Int. J. Adv. Sci. Eng. Inf. Technol. **7**(6), 2328–2336 (2017)
15. S. Neethirajan, Recent advances in wearable sensors for animal health management. Sens. Bio-Sens. Res **12**(44), 15–29 (2017)
16. A. Phaneuf, Latest trends in medical monitoring devices and wearable health technology. (Business Insider, 2019)
17. Heart health notifications on your Apple Watch, Apple, https://support.apple.com/en-us/HT208931. Accessed 25 Dec. 2021
18. A. Kos, V. Milutinović, A. Umek, Challenges in wireless communication for connected sensors and wearable devices used in sport biofeedback applications. Futur. Gener. Comput. Syst. **92**, 582–592 (2019)
19. H. Jahankhani, J. Ibarra, Digital forensic investigation for the Internet of Medical Things (IoMT). J. Forensic Leg. Investig. Sci. **5** (029) (2019)
20. O. AlShorman, B. AlShorman, M. Al-khassaweneh, F. Alkahtani, A review of internet of medical things (IoMT)—based remote health monitoring through wearable sensors: a case study for diabetic patients. Indones. J. Electr. Eng. Comput. Sci. **20**(1), 414–422 (2020)
21. Medical Device Radiocommunications Service (MedRadio), Federal Communications Commission, https://www.fcc.gov/medical-device-radiocommunications-service-medradio. Accessed 25 Dec. 2021
22. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the Internet of Medical Things (IoMT) systems security. IEEE Internet Things J. **8**(11), 8707–8718 (2020)
23. I.U. Din, M. Guizani, S. Hassan, B.-S. Kim, M.K. Khan, M. Atiquzzaman, S.H. Ahmed, The Internet of Things: a review of enabled technologies and future challenges. IEEE Access **7**, 7606–7640 (2018)
24. F.S.D. Lima Filho, F.A. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, L.F. Silveira, Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Secur. Commun. Netw. (2019)
25. P. Kasyoka, M. Kimwele, S. MbanduAngolo, Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. J. Med. Eng. Technol. **44**(1), 12–19 (2020)
26. T. Belkhouja, S. Sorour, M.S. Hefeida, Role-based hierarchical medical data encryption for implantable medical devices, in *2019 IEEE Global Communications Conference (GLOBECOM)*, 9–13 Dec. 2019, (2019), pp. 1–6
27. M. Papaioannou, M. Karageorgou, G. Mantas,V. Sucasas, I. Essop, J. Rodriguez, D. Lymberopoulos, A survey on security threats and countermeasures in Internet of Medical Things (IoMT), in *2019 IEEE Global Communications Conference (GLOBECOM)*, 9–13 Dec. (2019), pp. 1–6
28. A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*. (CRC Press, 2018)
29. J. Hash, P. Bowen, A. Johnson, C.D. Smith, D.I. Steinberg, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, Technology Administration (American Health Information Management Association, Illinois, 2008)
30. Talend, What is Data Integrity and Why Is It Important?, https://www.talend.com/resources/what-is-data-integrity/. Accessed 25 Dec. 2021
31. Y. Sun, F.P.-W. Lo, B. Lo, Security and privacy for the Internet of medical things enabled healthcare systems: a survey. IEEE Access **7**, 183339–183355 (2019)
32. T. Bienkowski, GDPR is explicit about protecting availability, https://www.netscout.com/blog/gdpravailability-protection (cit. on p. 18) (2018)

33. A. Alrawais, A. Alhothaily, C. Hu, X. Cheng, Fog computing for the Internet of Things: security and privacy issues. IEEE Internet Comput. **21**(2), 34–42 (2017)
34. R. Kumar, R. Tripathi, Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. J. Supercomput. **77**, 7916–7955 (2021)
35. J.P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, Securing internet of medical things systems: limitations, issues and recommendations. Futur. Gener. Comput. Syst. **105**, 581–606 (2020)
36. J.S. Lee, C.C. Chang, K.J. Wei, Provably secure conference key distribution mechanism preserving the forward and backward secrecy. Int. J. Netw. Secur. **15**(5), 405–410 (2013)
37. A. Abusukhon, N.M. Anwar, Z. Mohammad, B. Alghannam, A hybrid network security algorithm based on Diffie Hellman and Text to Image Encryption algorithm. J. Discret. Math. Sci. Cryptogr. **22**(1), 65–81 (2019)
38. J. Batamuliza, D. Hanyurwimfura, A secure and efficient anonymous certificateless signcryption for key distribution scheme for smart grid, in *2020 21st International Arab Conference on Information Technology (ACIT)* (IEEE, 2020), pp. 1–7
39. N. Park., M. Kim, H.C. Bang, Symmetric key-based authentication and the session key agreement scheme in IoT environment, in *Computer Science and its Applications*. Springer, Berlin, Heidelberg, (2015) pp. 379–384.
40. Casey Crane, Asymmetric versus symmetric encryption: definitions & differences, https://www.thesslstore.com/blog/asymmetric-vs-symmetric-encryption/. Accessed 25 Dec. 2021
41. V.H. Tutari, B. Das, D.R. Chowdhury, A continuous role-based authentication scheme and data transmission protocol for implantable medical devices. In *2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*, 25–28 Feb. 2019, (2019), pp. 1–6.
42. M.J. Marin-Jiménez, F.M. Castro, N. Guil, F. De la Torre, R. Medina-Carnicer, Deep multitask learning for gait-based biometrics, in *2017 IEEE International Conference on Image Processing (ICIP)* (IEEE, 2017), pp. 106–110.
43. S. Azad, A.-S.K. Pathan, *Practical Cryptography: Algorithms and Implementations Using C++*. ISBN: 978-1-48-222889-2, (CRC Press, Taylor & Francis Group, USA, 2014)
44. K. Juretus, I. Savidis, Reducing logic encryption overhead through gate level key insertion, in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, 22–25 (2016). https://doi.org/10.1109/ISCAS.2016.7538898
45. B.A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. Wireless Pers. Commun. **177**(1), 47–69 (2020)
46. Z. Xu, C. Xu, W. Liang, J. Xu, H. Chen, A lightweight mutual authentication and key agreement scheme for medical Internet of Things. IEEE Access **7**, 53922–53931 (2019)
47. S.B. Sadkhan, F.H. Abdulraheem, A proposed ANFIS evaluator for RSA cryptosystem used in cloud networking, in *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, 26–27 April 2017, https://doi.org/10.1109/CRCSIT.2017.7965561
48. A.A. Shaikh, N.S. Vani, An extended approach for securing the Short Messaging Services of GSM using multi-threading elliptical curve cryptography, in *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, 15–17 Jan. (2015), https://doi.org/10.1109/ICCICT.2015.7045733.
49. V.J. Jariwala, D.C. Jinwala, Chapter 4—adaptableSDA: secure data aggregation framework in wireless body area networks, in *Wearable and Implantable Medical Devices*, eds. by N. Dey, A. S. Ashour, S. James Fong, C. Bhatt, vol 7 (Academic Press, 2020), pp. 79–114
50. T. Bhatia, A.K. Verma, G. Sharma, Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing. Concurr. Comput.: Pract. Exp. **32**(5), 1–16 (2020)
51. K.E. Makkaoui, A. Beni-Hssane, A. Ezzati, Can hybrid homomorphic encryption schemes be practical?, in *2016 5th International Conference on Multimedia Computing and Systems (ICMCS)*, 29 Sept.–1 Oct. (2016), https://doi.org/10.1109/ICMCS.2016.7905580

52. G. Kalyani, S. Chaudhari, An efficient approach for enhancing security in Internet of Things using the optimum authentication key. Int. J. Comput. Appl. **42**(3), 306–314 (2020)
53. G.M. Abdullah, Q. Mehmood, C.B.A. Khan, Adoption of lamport signature scheme to implement digital signatures in IoT, in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 3–4 March (2018), https://doi.org/10.1109/ICOMET.2018.8346359
54. C. Easttom, N. Mei, Mitigating implanted medical device cyber security risks, in *IEEE 10th Annual Ubiquitous Computing. Electronics & Mobile Communication Conference (UEMCON)*, vol. 2019 (2019), pp. 0145–0148
55. Z.A. Alizai, N.F. Tareen, I. Jadoon, Improved IoT device authentication scheme using device capability and digital signatures, in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)* (IEEE, 2018) pp. 1–5
56. A. Kumari, S. Jangirala, M.Y. Abbasi, V. Kumar, M. Alam, ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. J. Inf. Secur. Appl. **51**, 1–12 (2020)
57. G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M.A. Orgun, S.C. Mukhopadhyay, Finger-to-Heart (F2H): authentication for wireless implantable medical devices. IEEE J. Biomed. Health Inform. **23**(4), 1546–1557 (2019)
58. G. Zheng, W. Yang, M. Johnstone, R. Shankaran, C. Valli, Securing the elderly in cyberspace with fingerprints, in *Assistive Technology for the Elderly*, eds. by N.K. Suryadevara, S.C. Mukhopadhyay (Academic Press, 2020) pp. 59–79
59. M. Dammak, O.R.M. Boudia, M.A. Messous, S.M. Senouci, C. Gransart, Token-based lightweight authentication to secure IoT networks, in *16th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (IEEE, 2019), pp. 1–4
60. W. Youssef, A.O. Zaid, M.S. Mourali, M.H. Kammoun, RFID-based system for secure logistic management of implantable medical devices in Tunisian health centers, in *2019 IEEE International Smart Cities Conference (ISC2)* (2019), pp. 83–86
61. A. Bhawiyuga, M. Data, A. Warda, Architectural design of token based authentication of MQTT protocol in constrained IoT device, in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (IEEE, 2017), pp. 1–4
62. S. Saif, S. Biswas, S. Chattopadhyay, Intelligent, secure big health data management using deep learning and blockchain technology: an overview, in *Deep Learning Techniques for Biomedical and Health Informatics*, eds. by S. Dash, B. Acharya, M. Mittal, A. Abraham, A. Kelemen, vol 68 (Springer International Publishing, Cham, 2020) pp. 187–209
63. A.A. Hady, A. Ghubaish, T. Salman, D. Unal, R. Jain, Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access **8**, 106576–106584 (2020)
64. L. Gupta, T. Salman, M. Zolanvari, A. Erbad, R. Jain, Fault and performance management in multi-cloud virtual network services using AI: a tutorial and a case study. Comput. Netw. **165**, 106950 (2019)
65. M.M. Ahemd, M.A. Shah, A. Wahid, Iot security: a layered approach for attacks and defenses, in *2017 International Conference on Communication Technologies (ComTech)* (IEEE, 2017) pp. 104–110
66. D. Antonioli, N.O. Tippenhauer, K. Rasmussen, BIAS: bluetooth impersonation attacks, in *IEEE Symposium on Security and Privacy (SP)*. (IEEE, 2020), pp. 549–562
67. I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of things: security vulnerabilities and challenges, in *IEEE Symposium on Computers and Communication (ISCC)*. (IEEE, 2015), pp. 180–187
68. F.-X. Standaert, Introduction to side-channel attacks, in *Secure Integrated Circuits and Systems* (Springer, Boston, MA, 2010), pp. 27–42
69. S. Maji, U. Banerjee, S.H. Fuller, M.R. Abdelhamid, P.M. Nadeau, R.T. Yazicigil, A.P. Chandrakasan, A low-power dual-factor authentication unit for secure implantable devices, in *2020 IEEE Custom Integrated Circuits Conference (CICC)* (2020), pp. 1–4
70. X. Chen, H. Zhu, D. Geng, W. Liu, R. Yang, S. Li, Merging RFID and blockchain technologies to accelerate big data medical research based on physiological signals. J. Healthc. Eng. 1–17 (2020)

71. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, C. Douligeris, Security in iomt communications: a survey. Sensors **20**(17), 4828 (2020)
72. M.N. Aman, K.C. Chua, B. Sikdar, A light-weight mutual authentication protocol for iot systems, in *GLOBECOM 2017–2017 IEEE Global Communications Conference* (2017), pp. 1–6
73. T. Gomes, F. Salgado, A. Tavares, J. Cabral, Cute mote, a customizable and trustable end-device for the internet of things. IEEE Sens. J. **17**(20), 6816–6824 (2017)
74. S. Sicari, A. Rizzardi, D. Miorandi, A. Coen-Porisini, Reato: reacting to denial of service attacks in the internet of things. Comput. Netw. **137**, 37–48 (2018)
75. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications. Int. J. Distrib. Sens. Netw. **10**(7), 1–15 (2014)
76. X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks on implantable medical devices, in *IEEE Global Telecommunications Conference GLOBECOM 2010*. (IEEE, 2010), pp. 1–5
77. S.C. Sethuraman, V. Vijayakumar, S. Walczak, Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. J. Med. Syst. **44**(1), 1–10 (2020)
78. Rambus, Industrial iot: Threats and countermeasures, https://www.rambus.com/iot/industrial-iot/. Accessed 25 Dec. 2021
79. P. Kukielka, Z. Kotulski, New Unknown Attack Detection with the Neural Network–Based IDS, in *Chapter 11, The State of the Art in Intrusion Prevention and Detection*, ed. by A.-S.K. Pathan. ISBN 9781482203516 (CRC Press, Taylor & Francis Group, USA, 2014)
80. O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, Y. Oren, Opening Pandora's Box: Effective Techniques for Reverse Engineering IoT Devices, in *International Conference on Smart Card Research and Advanced Applications* (Springer, Cham, 2017), pp. 1–21
81. F. I. Khan, S. Hameed, Understanding security requirements and challenges in internet of things (iots): a review, arXiv:1808.10529 (2018)
82. H. Ding, J. Han, Y. Zhang, F. Xiao, W. Xi, G. Wang, Z. Jiang, Preventing unauthorized access on passive tags, in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, Honolulu, HI, USA, IEEE, 16–19 April 2018, pp. 1115–1123
83. D. Zheng, A. Wu, Y. Zhang, Q. Zhao, Efficient and privacy-preserving medical data sharing in internet of things with limited computing power. IEEE Access **6**, 28019–28027 (2018)
84. U. Guin, A. Singh, M. Alam, J. Canedo, A. Skjellum, A secure low-cost edge device authentication scheme for the internet of things, in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)* (IEEE, 2018) pp. 85–90
85. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surveys Tutor. **17**(4), 2347–2376 (2015)
86. S. Deshmukh, S.S. Sonavane, Security protocols for Internet of Things: a survey, in *Proceedings of the 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)*, Chennai, India, 23–25 March 2017, pp. 71–74
87. M. Bagga, P. Thakral, T. Bagga, A Study on IoT: Model, Communication Protocols, Security Hazards & Countermeasures, in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (IEEE, 2018), pp. 591–598
88. K. Devadiga, IEEE 802.15.4 and the Internet of Things, Technical Report; Aalto University School of Science: Espoo, Finland, 2011. https://wiki.aalto.fi/download/attachments/59704179/devadiga-802-15-4-and-the-iot.pdf?version=1
89. R. Jain, *Wireless Protocols for IoT Part I: Bluetooth and Bluetooth Smart*. (Washington University in Saint Louis, Saint Louis, MO, USA, 2016). https://www.cse.wustl.edu/~jain/cse574-16/ftp/j_11ble.pdf
90. H. Javdani, H. Kashanian, Internet of things in medical applications with a service-oriented and security approach: a survey. Health Technol. **8**(1), 39–50 (2018)

91. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, RFID technology for IoT-based personal healthcare in smart spaces. IEEE Internet Things J. **1**(2), 144–152 (2014)
92. GS1, EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface, GS1: Brussels, Belgium, (2015) pp. 1–152, https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf. Accessed 25 Dec. 2021
93. L.M. Dang, M.J. Piran, D. Han, K. Min, H. Moon, A survey on internet of things and cloud computing for healthcare. Electronics **8**(7), 768 (2019)
94. Proceedings of the First ACM Conference on Wireless Network Security, WiSec '08, Alexandria, VA, USA, 31 March–2 April 2008; Association for Computing Machinery, New York, NY, USA (2008) pp. 140–147
95. D.Z. Sun, J.D. Zhong, hash-based RFID security protocol for strong privacy protection. IEEE Trans. Consum. Electron. **58**(4), 1246–1252 (2012)
96. I. Cvitic, M. Vujic, S. Husnjak, Classification of security risks in the IoT environment, in *Proceedings of the Annals of DAAAM and Proceedings of the International DAAAM Symposium*, Vienna, Austria, 21–24 October 2015 (2015) pp. 731–740
97. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019)
98. ECMA International, Near Field Communication-Interface and Protocol (NFCIP-1), ECMA International: Geneva, Switzerland, (2013) pp. 52, https://www.ecma-international.org/wp-content/uploads/ECMA-340_3rd_edition_june_2013.pdf. Accessed 25 Dec. 2021
99. H. Eun, H. Lee, H. Oh, Conditional privacy preserving security protocol for NFC applications. IEEE Trans. Consum. Electron. **59**(1), 153–160 (2013)
100. G. Madlmayr, J. Langer, C. Kantner, J. Scharinger, NFC Devices: Security and Privacy, in *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, Barcelona, Spain, 4–7 March 2008, pp. 642–647.
101. N.E. Tabet, M.A. Ayu, Analysing the security of NFC based payment systems, in *Proceedings of the 2016 International Conference on Informatics and Computing (ICIC)*, Mataram, Indonesia, 28–29 October (2016) pp. 169–174
102. Cypress. PSoC® Creator Component Datasheet-Bluetooth Low Energy (BLE) 3.10, Description SIG adopted Profiles and Services Comprehensive APIs, (2015) pp. 408–943, https://www.cypress.com/file/232821/download. Acessed 25 Dec. 2021
103. J.B. SIG, Bluetooth Specification, v. 3.0. EEE Spectr. (2009)
104. M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2018)
105. A.M. Lonzetta, P. Cope, J. Campbell, B.J. Mohd, T. Hayajneh, Security vulnerabilities in Bluetooth technology as used in IoT. J. Sens. Actuator Netw. **7**(3), 28 (2018)
106. G. Choudhary, A.K. Jain, Internet of Things: A survey on architecture, technologies, protocols and challenges, in *Proceedings of the 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Jaipur, India, 23–25 December 2016, pp. 1–8
107. C.W. Badenhop, S.R. Graham, B.W. Ramsey, B.E. Mullins, L.O. Mailloux, The Z-Wave routing protocol and its security implications. Comput. Secur. **68**, 112–129 (2017)
108. M.B. Yassein, W. Mardini, T. Almasri, Evaluation of security regarding Z-Wave wireless protocol, in *Proceedings of the Fourth International Conference on Engineering & MIS 2018*, Istanbul, Turkey, 9–11 April 2018; Association for Computing Machinery: New York, NY, USA, (2018) pp. 1–8
109. S.R. Ramson, D.J. Moni, A case study on different wireless networking technologies for remote health care. Intell. Decis. Technol. **10**(4), 353–364 (2016)
110. H. Fotouhi, A. Causevic, K. Lundqvist, M. Björkman, Communication and security in health monitoring systems–a review, in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. vol. 1 (IEEE, 2016), pp. 545–554
111. A. Chehri, H.T. Mouftah, Internet of Things-integrated IR-UWB technology for healthcare applications. Concurr. Comput.: Pract. Exp. **32**(2) (2020), e5454

112. W. Yin, X. Yang, L. Zhang, E. Oki, ECG monitoring system integrated with IR-UWB radar based on CNN. IEEE Access **4**, 6344–6351 (2016)
113. X. Zhang, M. Wei, P. Wang, Y. Kim, Research and implementation of security mechanism in ISA100.11a networks, in *Proceedings of the 2009 9th International Conference on Electronic Measurement Instruments*, Beijing, China, IEEE, 16–19 August 2009, pp. 4–716–4–721
114. Y. Zeng, J. Cao, J. Hong, S. Zhang, L. Xie, Secure localization and location verification in wireless sensor networks: a survey. J. Supercomput. **64**, 685–701 (2013)
115. Y. Wang, X. Ma, G. Leus, An UWB ranging-based localization strategy with internal attack immunity, in *Proceedings of the 2010 IEEE International Conference on Ultra-Wideband*, Nanjing, China, IEEE, 2(2010) pp. 1–4
116. M. Flury, M. Poturalski, P. Papadimitratos, J.P. Hubaux, J.Y. Le Boudec, Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging, in *Proceedings of the 3rd ACM Conference on Wireless Network Security, WiSec'10*, Hoboken, NJ, USA, 22–24 March 2010, pp. 117–128
117. M. Singh, P. Leu, S. Capkun, UWB with pulse reordering: securing ranging against relay and physical-layer attacks, in *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*, San Diego, CA, USA, 24–27 February 2019
118. S. Sundaresan, R. Doss, W. Zhou, RFID in Healthcare–Current Trends and the Future, in *Mobile Health* (Springer, Berlin/Heidelberg, Germany, 2015), pp. 839–870
119. S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in *Security in Pervasive Computing* (Springer, Berlin/Heidelberg, Germany, 2004), pp. 201–212
120. S. Upson, RFID Systems May Disrupt the Function of Medical Devices, IEEE Spectr, 2008, https://spectrum.ieee.org/computing/embedded-systems/rfid-systems-may-disrupt-the-function-of-medical-devices. Accessed 25 Dec. 2021
121. M. Roland, J. Langer, J. Scharinger, Applying relay attacks to Google Wallet, in *Proceedings of the 2013 5th International Workshop on Near Field Communication (NFC)*, Zurich, Switzerland, 5 February 2013, pp. 1–6
122. E. Haselsteiner, K. Breitfuß, Security in Near Field Communication (NFC) Strengths and Weaknesses (2006)
123. J. Dunning, Taming the blue beast: a survey of bluetooth based threats. IEEE Secur. Priv. **8**(2), 20–27 (2010)
124. LeCroy, CATC Merlin II-Bluetooth V1.2 Protocol Analyzer, LeCroy, Santa Clara, CA, USA, 2003, http://cdn.teledynelecroy.com/files/pdf/lecroy_merlinii_datasheet.pdf. Accessed 25 Dec. 2021
125. K.M. Haataja, K. Hypponen, Man-in-the-middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures, in *Proceedings of the 2008 3rd International Symposium on Communications, Control and Signal Processing*, St Julians, Malta, 12–14 March 2008, pp. 1096–1102
126. N.B.N.I. Minar, M. Tarique, Bluetooth security threats and solutions: a survey. Int. J. Distrib. Parallel Syst. **3**(1) (2012), 127
127. B. Fouladi, S. Ghanoun, SensePost UK Honey, i'm home!!, hacking zwave home automation systems, Black Hat USA, Las Vegas, Nevada, 2013, https://code.google.com/archive/p/z-force/. Accessed 25 Dec. 2021
128. P. Sarigiannidis, E. Karapistoli, A.A. Economides, Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. Expert Syst. Appl. **42**(21), 7560–7572 (2015)
129. A. Compagno, M. Conti, A.A. D'Amico, G. Dini, P. Perazzo, L. Taponecco, Modeling enlargement attacks against UWB distance bounding protocols. IEEE Trans. Inf. Forensics Secur. **11**(7), 1565–1577 (2016)
130. N. Vidgren, K. Haataja, J.L. Patiño-Andres, J.J. Ramírez-Sanchis, P. Toivanen, Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned, in *Proceedings of the Annual Hawaii International Conference on System Sciences*, Wailea, HI, USA, vol. 7–10 (2013), pp. 5132–5138

131. M.R. Fuentes, N. Huq, Securing connected hospitals, by Trend Micro, 2018, https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf. Accessed 25 Dec. 2021
132. T. Poongodi, A. Rathee, R. Indrakumari, P. Suresh, IoT Sensing Capabilities: Sensor Deployment and Node Discovery, Wearable Sensors, Wireless Body Area Network (WBAN), data acquisition, in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm.* ed. by S.L. Peng, S. Pal, L. Huang (Springer International Publishing, Cham, Switzerland, 2020), pp. 127–151
133. M. Sain, Y.J. Kang, H.J. Lee, Survey on security in Internet of Things: state of the art and challenges, in *Proceedings of the International Conference on Advanced Communication Technology, ICACT*, vol. 19–22 (IEEE, Bongpyeong, Korea, 2017), pp. 699–704
134. T. Salman, R. Jain, A Survey of Protocols and Standards for Internet of Things, arXiv 2019, arXiv:1903.11549
135. G. Calcagnini, E. Mattei, F. Censi, M. Triventi, R. Lo Sterzo, E. Marchetta, P. Bartolini, Electromagnetic compatibility of WiFi technology with life-supporting medical devices, in *Proceedings of the World Congress on Medical Physics and Biomedical Engineering*, Munich, Germany, 7–12 September 2009 (Springer, Berlin/Heidelberg, Germany, 2009), pp. 616–619
136. B.A. Mubdir, H.M.A. Bayram, Adopting MQTT for a multi protocols IoMT system. Int. J. Electr. Comput. Eng. *12*(1), 2088–8708 (2022)
137. H. Peng, WIFI network information security analysis research, in *Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, IEEE, 21–23 April 2012, pp. 2243–2245
138. M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: a block architecture. IEEE Access **6**, 32700–32726 (2018)
139. D.C. Yacchirema, C.E. Palau, M. Esteve, Enable IoT interoperability in ambient assisted living: active and healthy aging scenarios, in *Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 8–11 January 2017, pp. 53–58
140. Zigbee Alliance Inc, ZigBee Specification, Zigbee Alliance Inc. (2015), pp. 1–378, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf. Accessed on 25 Dec. 2021
141. S. Plosz, A. Farshad, M. Tauber, C. Lesjak, T. Ruprechter, N. Pereira, Security vulnerabilities and risks in industrial usage of wireless communication, in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, Barcelona, Spain, IEEE, 16–19 September 2014.
142. O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen, Three practical attacks against ZigBee security: attack scenario definitions, practical experiments, countermeasures, and lessons learned, in *Proceedings of the 2014 14th International Conference on Hybrid Intelligent Systems*, Hawally, Kuwait, 14–16 December 2014, pp. 199–206
143. S.M. Rana, M.A., Halim, M.H. Kabir, Design and implementation of a security improvement framework of Zigbee network for intelligent monitoring in IoT platform. Appl. Sci. **8**(11), 2305 (2018)
144. T. Zhong, C. Mengjin, Z. Peng, W. Hong, Real-time communication in WIA-PA industrial wireless networks, in *Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, China, 9–11 July 2010, Vol 2, pp. 600–605
145. C.R. Su, J. Hajiyev, C.J. Fu, K.C. Kao, C.H. Chang, C.T. Chang, A novel framework for a remote patient monitoring (RPM) system with abnormality detection. Health Policy Technol. **8**(2), 157–170 (2019). https://doi.org/10.1016/j.hlpt.2019.05.008
146. X. Wang, L. Cui, Z. Guo, Advanced technologies in ad hoc and sensor networks, in *Proceedings of the 7th China Conference on Wireless Sensor Networks*, vol. 295 (2014), pp. 288
147. W. Liang, X. Zhang, Y. Xiao, F. Wang, P. Zeng, H. Yu, Survey and experiments of WIA-PA specification of industrial wireless network. Wirel. Commun. Mob. Comput. **11**(8), 1197–1212 (2011)

148. W. Min, X. Zhang, W. Ping, K. Kim, Y. Kim, Research and implementation of the security method based on WIA-PA standard, in *Proceedings of the 2010 International Conference on Electrical and Control Engineering*, Wuhan, China, 25–27 June 2010, pp. 1580–1585
149. H. Fotouhi, A. Cauševic, M. Vahabi, M. Björkman, Interoperability in heterogeneous low-power wireless networks for health monitoring systems, in *Proceedings of the 2016 IEEE International Conference on Communications Workshops (ICC)*, Kuala Lumpur, Malaysia, 23–27 May 2016, pp. 393–398
150. J. Olsson, 6LoWPAN Demystified, Texas Instruments: Dallas, TX, USA, 13 (2014), https://www.ti.com/lit/wp/swry013/swry013.pdf?ts=1645202797751&ref_url=https%253A%252F%252Fwww.google.com%252F. Accessed 25 Dec. 2021
151. P. Chen, Yokogawa electric corporation, using ISA100.11a wireless technology to monitor pressure and temperature in a refinery (2011)
152. Y. Benslimane, K. Benahmed, H. Benslimane, Security mechanisms for 6LoWPAN network in context of Internet of Things: a survey, in *Renewable Energy for Smart and Sustainable Cities*, ed. by M. Hatti (Springer International Publishing, Cham, Switzerland, 2019), pp. 49–69
153. i-Scoop, LoRa and LoRaWAN: the technologies, ecosystems, use cases and market by i-Scoop, https://www.i-scoop.eu/internet-of-things-guide/lpwan/iot-network-lora-lorawan/. Accessed 25 Dec. 2021
154. J. Haxhibeqiri, E. De Poorter, I. Moerman, J. Hoebeke, A survey of LoRaWAN for IoT: from technology to application. Sensors **18**(11), 3995 (2018)
155. A. Mdhaffar, T. Chaari, K. Larbi, M. Jmaiel, B. Freisleben, IoT-based health monitoring via LoRaWAN, in *Proceedings of the IEEE EUROCON 2017–17th International Conference on Smart Technologies*, Ohrid, Macedonia, 6–8 July 2017, pp. 519–524
156. P.A. Catherwood, D. Steele, M. Little, S. Mccomb, J. Mclaughlin, A community-based IoT personalized wireless healthcare solution trial. IEEE J. Transl. Eng. Health Med. **6**, 1–13 (2018)
157. A. Gemalto, Semtech, LoRaWAN™ security a white paper prepared for the LoRa alliance, https://lora-alliance.org/sites/default/files/2019-05/lorawan_security_whitepaper.pdf. Accessed 25 Dec. 2021
158. A. Yegin, T. Kramp, P. Dufour, R. Gupta, R. Soss, O. Hersent, D. Hunt, N. Sornin, LoRaWAN protocol: specifications, security, and capabilities, in *LPWAN Technologies for IoT and M2M Applications*. ed. by B.S. Chaudhari, M. Zennaro (Academic Press, Cambridge, MA, USA, 2020), pp. 37–63
159. L.N. Whitehurst, T.R. Andel, J.T. McDonald, Exploring security in ZigBee networks, in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, Oak Ridge, TN, USA, 8–10 April 2014, pp. 25–28
160. E. Ronen, A. Shamir, A.O. Weingarten, C. O'Flynn, IoT goes nuclear: creating a ZigBee chain reaction, in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)*, CA, USA, 22–26 May 2017, pp.195–212
161. X. Cao, D.M. Shila, Y. Cheng, Z. Yang, Y. Zhou, J. Chen, Ghost-in-zigbee: energy depletion attack on zigbee-based wireless networks. IEEE Internet Things J **3**(5), 816–829 (2016)
162. Y. Qi, W. Li, X. Luo, Q. Wang, Security analysis of WIA-PA protocol, in *Advanced Technologies in Ad Hoc and Sensor Networks*, vol. 295 (Springer, Berlin/Heidelberg, Germany), pp. 287–298 (2014)
163. G. Glissa, A. Meddeb, 6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features, in *Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain, 26–30 June 2017, pp 264–269
164. J.-S. Lee., Y.-W. Su, C.-C. Shen, A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi, in *IECON 2007–33rd Annual Conference of the IEEE Industrial Electronics Society*, (IEEE, 2007), pp. 46–51
165. R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN fragmentation attacks and mitigation mechanisms, in *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec April 2013, Budapest, Hungary, 2013, pp. 55–66

166. X. Yang, E. Karampatzakis, C. Doerr, F. Kuipers, Security vulnerabilities in LoRaWAN, in *Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Orlando, FL, USA, 17–20 April 2018, IEEE, 2018, pp. 129–140
167. S.S. Arrieta, O.J.S. Parra, R.M.P. Chaves, Design of PHD solution based on HL7 and IoT, in *Future Data and Security Engineering*. ed. by T.K. Dang, J. Küng, R. Wagner, N. Thoai, M. Takizawa (Springer International Publishing, Cham, Switzerland, 2018), pp. 405–409
168. A.F. Santamaria, F. De Rango, A. Serianni, P. Raimondo, A real IoT device deployment for e-Health applications under lightweight communication protocols, activity classifier and edge data filtering. Comput. Commun. **128**, 60–73 (2018)
169. J. Hong, P. Morris, J. Seo, Interconnected personal health record ecosystem using IoT cloud platform and HL7 FHIR, in *Proceedings of the 2017 IEEE International Conference on Healthcare Informatics (ICHI)*, Park City, UT, USA, 23–26 August 2017, pp. 362–367
170. A. Duggal, HL7 2. x security, in *Proceedings of the The 8th Annual HITB Security Conference*, Amsterdam, The Nertherlands, 10–14 April 2017
171. C. Gündoğan, P. Kietzmann, M. Lenders, H. Petersen, T.C. Schmidt, M. Wählisch, NDN, CoAP, and MQTT: a comparative measurement study in the IoT, in *Proceedings of the 5th ACM Conference on Information-Centric Networking* (2018), pp. 159–171
172. A. Hussain, T. Ali, F. Althobiani, U. Draz, M. Irfan, S. Yasin, S. Shafiq, Z. Safdar, A. Glowacz, G. Nowakowski, M.S. Khan, S. Alqhtani, Security framework for IoT based real-time health applications. Electronics **10**(6), 719 (2021)
173. S.N. Swamy, D. Jadhav, N. Kulkarni, Security threats in the application layer in IOT applications, in *Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 10–11 February 2017, pp. 477–480
174. M. Brachmann, O. Garcia-Morchon, M. Kirsche, Security for practical coap applications: Issues and solution approaches, in *GI/ITG KuVS Fachgesprch Sensornetze (FGSN), Paderborn* (University Stuttgart, Stuttgart, Germany, 2011)
175. T. Dey, S. Jaiswal, S. Sunderkrishnan, N. Katre, HealthSense: a medical use case of Internet of Things and Blockchain, in *Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, India, 7–8 December 2017, pp. 486–491
176. V. Karagiannis, P. Chatzimisios, F. Vazquez-gallego, J. Alonso-zarate, Sensus: smart water network, rans. IoT Cloud Comput. **3**, 1–10 (2016)
177. G. Suciu, V. Suciu, A. Martian, R. Craciunescu, A. Vulpe, I. Marcu, S. Halunga, O. Fratu, Big data, internet of things and cloud convergence—an architecture for secure e-health applications. J. Med. Syst. **39**(11), 1–8 (2015)
178. Y. Liu, G. Zhang, W. Chen, X. Wang, An efficient privacy protection solution for smart home application platform, in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, China, IEEE, (2016), pp. 2281–2285
179. J.F. Reschke, The 'basic' http authentication scheme, in *Internet Engineering Task Force (IETF) Internet Engineering Steering Group (IESG) 2015*. https://httpwg.org/specs/rfc7617.html, Accessed 25 Dec. 2021
180. R.A. Rahman, B. Shah, Security analysis of IoT protocols: a focus in CoAP, in *Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, Muscat, Oman, 15–16 March 2016, pp. 1–7
181. S. Arvind, V.A. Narayanan, An overview of security in CoAP: attack and analysis, in *Proceedings of the 2019 5th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2019, pp. 655–660
182. D. Dinculeana, X. Cheng, Vulnerabilities and limitations of MQTT protocol used between IoT devices. Appl. Sci. **9**(5), 848 (2019)

183. S. Andy, B. Rahardjo, B. Hanindhito, Attack scenarios and security analysis of MQTT communication protocol in IoT system, in *Proceedings of the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Yogyakarta, Indonesia, 2017, pp. 1–6
184. D. Moustis, P. Kotzanikolaou, Evaluating security controls against HTTP-based DDoS attacks, in *Proceedings of the IISA*, 10–12 July 2013 (IEEE, Piraeus, Greece, 2013), pp. 1–6

Rachida Hireche has a computer engineer diploma in 2006 on parallel and distributed systems specialty from the University of Mentouri Brothers Constantine, Algeria. And Master diploma in 2019 on information and communications science and technology specialty from Abdelhafid Boussouf University Mila, Algeria. She is the manager of development service in the University of Abdelhafid Boussouf Mila since 2010. She is currently a Ph.D. candidate in computer sciences department, faculty of sciences, University of Farhat Abbes Setif 1, Algeria. Her research interests focus on Fault Tolerance and Security Management in Medical Internet of Things (IoMT).

Houssem Mansouri obtained the engineering degree in computer science from University of Farhat Abbes Setif 1, Algeria in 2004 and his master's degree in computer science from the University of Abderrahmane Mira Bejaia, Algeria in 2007. He received his Ph.D. on fault tolerance in mobile environment from the doctoral school in computer sciences of the University of Abderrahmane Mira Bejaia in 2016. He also obtained the diploma of "enabling to supervise research works" in 2019 from University of Farhat Abbes Setif 1. He is actually associate professor in computer science. He is working since 2008 until now as part-time lecturer at the computer science department in faculty of sciences, Farhat Abbes Setif 1, where he held the position of academic deputy chairman of computer science department from 2010 to 2014 and the position of Head of E-learning Unit between 2015 and 2020. He is the head of the laboratory of networks and distributed systems since 2021. His research interests are fault tolerance and security in networks and distributed systems.

Al-Sakib Khan Pathan is a Professor at Computer Science and Engineering department, United International University (UIU), Bangladesh. He is also serving as a Ph.D. Co-supervisor (external) at Computer Sciences Department, University Ferhat Abbas Setif 1, Algeria. He received Ph.D. degree in Computer Engineering in 2009 from Kyung Hee University, South Korea and B.Sc. degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2003. In his academic career so far, he worked as a faculty member in various capacities in various institutions like at the CSE Department of Independent University, Bangladesh (IUB) during 2020–2021, Southeast University,

Bangladesh during 2015–2020, Computer Science department, International Islamic University Malaysia (IIUM), Malaysia during 2010–2015; at BRACU, Bangladesh during 2009–2010, and at NSU, Bangladesh during 2004–2005. He served as a Guest Professor at the Department of Technical and Vocational Education, Islamic University of Technology, Bangladesh in 2018. He also worked as a Researcher at Networking Lab, Kyung Hee University, South Korea from September 2005 to August 2009 where he completed his MS leading to PhD. His research interests include wireless sensor networks, network security, cloud computing, and e-services technologies. Currently he is also working on some multidisciplinary issues. He is a recipient of several awards/best paper awards and has several notable publications in these areas. So far, he has delivered 32 Keynotes and Invited speeches at various international conferences and events. He was named on the List of Top 2% Scientists of the World, 2019 and Top 2% Scientists on the World, 2020 by Stanford University, USA in 2020 and 2021. He has served as a General Chair, Organizing Committee Member, and Technical Program Committee (TPC) member in numerous top-ranked international conferences/workshops like INFOCOM, GLOBECOM, ICC, LCN, GreenCom, AINA, WCNC, HPCS, ICA3PP, IWCMC, VTC, HPCC, SGIoT, etc. He was awarded the IEEE Outstanding Leadership Award for his role in IEEE GreenCom'13 conference and IEEE Outstanding Service Awards twice in recognition and appreciation of the service and outstanding contributions to the IEEE IRI'20 and IRI'21. He is currently serving as the Editor-in-Chief of International Journal of Computers and Applications and Journal of Cyber Security Technology, Taylor & Francis, UK; Editor of Ad Hoc and Sensor Wireless Networks, Old City Publishing, International Journal of Sensor Networks, Inderscience Publishers, and Malaysian Journal of Computer Science, Associate Editor of Connection Science, Taylor & Francis, UK, International Journal of Computational Science and Engineering, Inderscience, Area Editor of International Journal of Communication Networks and Information Security, Guest Editor of many special issues of top-ranked journals, and Editor/Author of 30 books. One of his books has been included twice in Intel Corporation's Recommended Reading List for Developers, 2nd half 2013 and 1st half of 2014; 3 books were included in IEEE Communications Society's (IEEE ComSoc) Best Readings in Communications and Information Systems Security, 2013, several other books were indexed with all the titles (chapters) in Elsevier's acclaimed abstract and citation database, Scopus and in Web of Science (WoS), Book Citation Index, Clarivate Analytics, at least one has been approved as a textbook at NJCU, USA in 2020, one is among the Top Used resources on SpringerLink in 2020 for UN's Sustainable Development Goal 7 (SDG7)—Affordable and Clean Energy and one book has been translated to simplified Chinese language from English version. Also, 2 of his journal papers and 1 conference paper were included under different

categories in IEEE Communications Society's (IEEE ComSoc) Best Readings Topics on Communications and Information Systems Security, 2013. He also serves as a referee of many prestigious journals. He received some awards for his reviewing activities like: one of the most active reviewers of IAJIT several times; Elsevier Outstanding Reviewer for Computer Networks, Ad Hoc Networks, FGCS, and JNCA in multiple years. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), USA.