Early View e4049
SPECIAL ISSUE ARTICLE
Full Access

A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)

Maria Papaioannou

Corresponding Author

- m.papaioannou@av.it.pt
- orcid.org/0000-0003-3830-7190

Instituto de Telecomunicações, Aveiro, Portugal

Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

Correspondence

Maria Papaioannou, Instituto de Telecomunicações, Aveiro, Portugal.

Email: m.papaioannou@av.it.pt

Search for more papers by this author
Marina Karageorgou

Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

Search for more papers by this author
Georgios Mantas

Instituto de Telecomunicações, Aveiro, Portugal

Faculty of Engineering and Science, University of Greenwich, Greenwich, UK

Search for more papers by this author
Victor Sucasas

Instituto de Telecomunicações, Aveiro, Portugal

Search for more papers by this author
Ismael Essop

Faculty of Engineering and Science, University of Greenwich, Greenwich, UK

Search for more papers by this author
Jonathan Rodriguez

Instituto de Telecomunicações, Aveiro, Portugal

Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd, UK

Search for more papers by this author
Dimitrios Lymberopoulos

Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

Search for more papers by this author
Maria Papaioannou

Corresponding Author

- m.papaioannou@av.it.pt
- orcid.org/0000-0003-3830-7190

Instituto de Telecomunicações, Aveiro, Portugal

Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

Correspondence

Maria Papaioannou, Instituto de Telecomunicações, Aveiro, Portugal.

Email: m.papaioannou@av.it.pt

Search for more papers by this author
Marina Karageorgou

Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

Search for more papers by this author

Georgios Mantas

Instituto de Telecomunicações, Aveiro, Portugal

Faculty of Engineering and Science, University of Greenwich, Greenwich, UK

Search for more papers by this author
Victor Sucasas

Instituto de Telecomunicações, Aveiro, Portugal

Search for more papers by this author
Ismael Essop

Faculty of Engineering and Science, University of Greenwich, Greenwich, UK

Search for more papers by this author
Jonathan Rodriguez

Instituto de Telecomunicações, Aveiro, Portugal

Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd, UK

Search for more papers by this author
Dimitrios Lymberopoulos

Department of Electrical and Computer Engineering, University of Patras, Patras, Greece

Abstract

Internet of medical things (IoMT) is an emerging technology aiming to improve the patient's quality of life by enabling personalized e-health services without limitations on time and location. Nevertheless, IoMT devices (eg, medical sensors) that constitute the key underlying elements of the IoMT edge network are vulnerable to various types of security threats and thus, they pose a significant risk to patient's privacy and safety. Based on that and the fact that the security is a critical factor for the successful integration of IoMT technology into pervasive healthcare systems, there is an urgent need for novel security mechanisms to preserve the security of the IoMT edge network. Toward this direction, the first step is the comprehensive understanding of existing and potential threats to the IoMT edge network environment. Thus, in this article, we provide a categorization of security threats to the edge network environment based on the major security objectives that they target. Moreover, we present a categorization of security

countermeasures, derived from the literature, against threats to IoMT edge networks. The authors' intent is to provide a foundation for organizing research efforts toward the development of proper security countermeasures for protecting IoMT edge networks against internal and external threats.

1 INTRODUCTION

Nowadays, where time and space cease to have limits thanks to new technologies, services are on the same path. One of the areas considered to be pioneer in adopting technologies to provide real-time and ubiquitous services is the healthcare sector. Under the umbrella of Internet of things (IoT) a wide range of entities, including people, machines, and things are interconnected into information space in anywhere at any time.[1, 2] The evolution and rise of IoT are transforming the healthcare industry and introduce the Internet of medical things (IoMT), where medical devices are interconnected in a global network that anyone, anywhere, and anytime may have access to[3].

The landscape of e-health IoMT-based applications has taken a remarkable lead in terms of wellness services motivating millions of people around the world to achieve a healthier lifestyle. In this context, healthcare services have transformed into user-centric, precise, ubiquitous, and personalized services such as a private healthcare provider round the clock.[4-6] However, in order to achieve the maximum possible outcome from these healthcare applications over IoMT, certain challenges, which are just around the corner, need serious attention so as to be addressed.[7-9] In particular, IoMT devices (eg, medical wearable and implantable sensors) that constitute the key underlying elements of the IoMT edge network are vulnerable to various types of security threats and thus, they pose a significant risk to patient's privacy and safety. For example, adversaries can hack into IoMT devices themselves and modify the stored data or manipulate device's functionality. Based on that and the fact that security is a critical factor highly dependent on the reliability of the involved medical devices, for the successful deployment of IoMT technology into pervasive healthcare systems, there is an urgent need for novel security mechanisms to preserve the security of the IoMT edge network. To this end, the first step is the comprehensive understanding and proper categorization of existing and potential threats to the IoMT edge network environment. As IoMT devices have capabilities and technical characteristics similar to those of IoT devices, existing attacks against IoT networks can also be considered as potential threats to the IoMT edge network.[10] Therefore, the authors pursued an extensive research on the existing and potential security threats to the IoMT edge network environment and provide a categorization based on the major security objectives that these threats target. Moreover, the authors present a categorization of security countermeasures, derived from the literature, against threats to IoMT edge networks.

Following the Introduction, the rest of the article is organized as follows. In Section 2, a system architecture of IoMT-enabled healthcare systems is presented along with the definition of the IoMT edge network. The major security objectives in IoMT edge network are described in Section 3, while a detailed description of the generalized attack types in IoMT edge network is discussed in Section 4. Section 5presents a categorization of the security threats that have already been realized or can be potentially launched against IoMT edge network based on the major security objectives that they target. In Section 6, a categorization of security countermeasures addressing these threats, derived from the literature, is provided. Finally, the survey article is concluded in Section 7.

2 SYSTEM ARCHITECTURE OF IoMT-ENABLED HEALTHCARE SYSTEMS

IoMT is basically an IoT-based solution that enables the development of IoT-enabled healthcare systems for monitoring a variety of different kinds of vital signs such as ECG, heart rate, and blood pressure.[3] The key aspect in IoMT-enabled healthcare systems is to improve patients' quality of life by mitigating a possible unpleasant hospitalization.[11] Giving the patients the opportunity to walk around the medical and nonmedical environments and guaranteeing the continuously monitoring of their vital signs and health status, without any interruption, is a fundamental feature for high quality provision of medical services.[12-14]

The main component of an IoMT-based healthcare system is the IoMT edge network, as shown in Figure 1, consisting of a rich set of IoMT-enabled devices that enable the individuals to track their physical wellness and monitor their health status digitally.[15, 16] For instance, the individuals may monitor their health data any time, from any computer or mobile device. IoMT-enabled devices can vary from smart watches or smart shoes to a wide range of sensors such as ECG sensors, EEG sensors, airflow sensors, blood pressure sensors, motion sensors, and activity sensors as shown in Figure 1.[3, 12] It is noteworthy to mention that IoMT-enabled sensors have ubiquitous and pervasive identification, sensing, and communication capabilities so that vital signs can be captured from any place (eg, home, hospital, office).[12] Moreover, the IoMT edge network includes the user's terminal device (eg, smartphone) that plays the role of the smart e-health gateway. This gateway is responsible for receiving and forwarding the received vital sign data, based on the network availability, to either: (i) a cellular base station, through a long-range wireless technology (eg, 4G/5G), or (ii) a router, through short coverage communication protocols, such as Bluetooth and 6LoWPAN, or Wi-Fi, so that the vital sign data will reach, over the Internet, the Cloud platform services at the healthcare provider side for further data processing and storage.[3, 12] The collected health data may represent a source of big data for statistical and epidemiological research. The cloud services are accessible by the patients from anywhere and at

any time. At the same time, authorized healthcare professionals may access these services in order to provide medical diagnosis and treatment to the patients.

FIGURE 1
Open in figure viewerPowerPoint
System architecture of IoMT-enabled healthcare systems.

3 SECURITY OBJECTIVES IN IoMT EDGE NETWORK

In the context of the IoMT edge network, the following six major security objectives have been identified:

3.1 Confidentiality

Assures that confidential information is not made available or disclosed to unauthorized entities.[17] In the context of the IoMT edge network, confidentiality refers to the protection of patient's medical information, shared with a therapist, a physician or medical staff, from being disclosed to unauthorized third parties that can harm the patient or use this medical information in an inappropriate manner.[18] For example, if confidentiality of the transmitted data is not preserved, an adversary could interfere between the sender (eg, medical IoT device) and the receiver (eg, smartphone-gateway) in order to intercept the transmitted medical data and access unauthorized information. There is a wide range of approaches to ensure confidentiality ranging from physical protection to cryptographic algorithms which unintelligibly render data.[17]

3.2 Integrity

Assures that data have not been destroyed or altered in an unauthorized manner.[17] Applied to IoMT edge network, integrity preserves the accuracy of patient related information such as personal medical data, health summary, clinical notes, and test results.[17] In particular, the integration of the emerging IoT technology in the healthcare sector has been increasing the reliance upon networked data, and, more than ever, healthcare organizations realize the importance of data integrity. Apart from data integrity, in the context of the IoMT edge network, the concepts of device and software integrity have drawn attention as well. The successful acceptance of IoMT edge networks in healthcare sector is also highly dependent on the integrity of the involved devices such as wearable or implantable sensors.[19] However, due to the fact that IoMT devices usually operate in trustless environments, they are subject to physical attacks that target device integrity.[20] Besides, the integrity of the running software (eg, operating systems,

applications) on the medical devices is also a key element for ensuring security in the IoMT edge network.[20]

3.3 Non-repudiation

Prevents an entity from denying previous commitments or actions in an interaction.[17] For instance, data extracted from the sensors of one patient may send and later the patient deny such data belong to him. Or, an authorized developer updates the firmware in few sensors and afterward deny its validity. When disputes arise due to an entity denying previous commitments or certain actions that were authorized, there is a need for a means to resolve the situation. In many cases, a specific procedure involving a trusted third party is needed to resolve such disputes.[17]

3.4 Authentication

Applies to both entities (ie, entity authentication) and transmitted information (ie, message authentication).[17] Entity authentication or identification is the process by which one communicating entity is assured of the claimed identity of another entity involved in the interaction, and that the latter has actually participated. On the other hand, message authentication is the process by which an entity is verified as the original source of given data generated at some time in the past.[17] Nowadays, there is a trend toward lightweight authentication protocols as many IoT devices do not provide enough memory and CPU power to execute the cryptographic operations required for traditional authentication protocols.[21]

3.5 Authorization

Is the conveyance, to another entity, of official permission to do or be something.[17] In other words, authorization ensures that only entitled entities can obtain access to certain network services or resources, such as a medical IoT device or collected medical data of a patient. For instance, only trusted expertise parties are granted permission to perform a given action such as issuing commands to medical IoT devices, or updating the medical IoT device software.[21] Access control is a common security technique that ensures authorization.

3.6 Availability

Ensures that systems work properly and services are not denied to authorized users.[22] Therefore, medical data are always accessible and useable upon demand by a legitimate entity. In the context of IoMT edge network, it is of major importance to ensure the availability of device and network resources when a patient needs care services without disruptions.[23, 24]

4 GENERALIZED ATTACK TYPES IN IoMT EDGE NETWORK

The increasing number of resource-constrained medical devices connected to IoMT-based networks over wireless networks leads to security breaches by malicious actors who exploit possible system vulnerabilities in order to launch attacks and gain access to confidential information or affect extracted results and device operations.[25, 26] This section presents a brief description of generalized types of attacks that can be potential attacks against IoMT edge networks.

4.1 Eavesdropping attacks

An attack which takes advantage of unsecured network communications to interfere between the communication of two entities, such as smartphones or sensor nodes, without their consent. The attacker secretly listens to the communication to capture useful information, so afterward the attacker can use this information to masquerade as the claimant. Eavesdropping attacks are difficult to detect because they do not cause abnormalities to the network transmission operations.[27]

4.2 Spoofing attacks

The deliberate prompting of an entity or resource to act in an incorrect way. For instance, the attacker may fake the sending address of the transmission data in order to illegally enter into a secure system. Piggybacking and mimicking are being considered as types of spoofing.[27]

4.3 Traffic analysis attacks

A form of passive attack in which an intruder gains knowledge of the transmitted information by inference from observable characteristics of a data flow. The information may not be directly available, for instance, when the data are encrypted. These characteristics may include the identities and locations of the involved entities (ie, sources and destinations) of the data flow, and also the flow's presence, absence, amount, direction, frequency, and duration of occurrence.[27]

4.4 Masquerading attacks

A type of active attack whereby unauthorized entities illegitimately pose as authorized entities to gain greater privilege to a system than what they are authorized for. Moreover, the attacker may perform a malicious action by illegitimately posing as an authorized entity.[27] For instance, the attacker may steal the user's terminal device (eg, user's smartphone) login credentials and gain unauthorized privileges to access stored confidential health data by masquerading the legitimate user.[20]

4.5 Physical attacks

Physical attacks are concentrated on the physical layer, and so on the devices themselves.[28-30] For instance, adversary changes the behavior or structure of devices involved in IoMT edge network by leading the system to hardware failure.[22] Examples of physical attacks include device capture, tampering, invasive hardware attacks, side-channel attacks, and reverse engineering attacks.[20]

4.6 Malware attacks

An attacker designs and operates malicious software or firmware in order to violate the security of a system. This software or firmware is often covertly inserted into another program and intents to destroy data, run destructive or intrusive programs, or otherwise compromise the privacy, accuracy, or reliability of the system's data, applications, or the entire operating system. Common means for malware attacks include worms, virus programs, malicious mobile code, trojan horses, rootkits, or other code-based malicious entity that successfully infects a system.[27, 31]

4.7 Man-in-the-middle attacks

This kind of active attack takes place when a malicious actor interferes in the communication between two authenticated entities (eg, the claimant and verifier of the authentication protocol), intercepting, compromising, or even concealing messages exchanged to each other. The attacker may selectively alter the communicated data to masquerade as one or more of the legitimate entities involved.[32]

4.8 Denial-of-service attacks

A type of attack aiming at the obstruction of provisioning time-critical functions or the restriction of accessing authorized assets and facilities.[33, 34] Time-critical may be milliseconds or it may be hours, depending upon the service provided. This could be achieved by flooding the resource constrained IoMT edge network with a great number of requests, causing bandwidth congestion.[35, 36]

4.9 Battery drainage attacks

Battery drainage attack occurs when an adversary exploits the resource constraints of a device (ie, mostly a wearable or an implantable one) in order to drain its battery and make it unavailable for the legitimate user.[37, 38] For example, the attacker may overrun the IoMT device with a large number of no authorized requests thus preventing it from going to sleep or energy saving mode.[20]

4.10 Impersonation attacks

Another type of attack is impersonation where a malicious actor pretends to be a legitimate entity (eg, Claimant or Verifier) in an authentication protocol in order to gain access to resources to which they are not authorized for Reference 39. In the scenario where the attacker impersonates the Verifier in an authentication protocol, he/she usually aims to capture information about the Claimant that can be used to impersonate as a Claimant to the real Verifier.[27]

4.11 Message fabrication/modification/replay attacks

Finally, in message fabrication/modification and replay attacks the adversary is able to construct, change, or resend, respectively, already transmitted messages between legitimate entities with the intent of producing an unauthorized effect or gaining unauthorized access.[40]

5 SECURITY THREATS IN IoMT EDGE NETWORK

In IoMT edge network environment, where the transmitted, processed, and stored data are sensitive, the concerns about security and privacy are increased.[41] Therefore, at this section, the authors provide a categorization of the security threats, as shown in Figure 2 targeting the IoMT edge network based on the security objectives that they intend to compromise.

FIGURE 2
Open in figure viewerPowerPoint
Categorization of security threats in IoMT edge network.

5.1 Security threats to data confidentiality

IoMT edge network consists of resource-constrained IoT devices which deter the use of resource-demanding cryptographic solutions (eg, data encryption/decryption) ensuring high level of data confidentiality, and thus making the network vulnerable to threats targeting the confidentiality of the exchanged or stored data.[21] For example, an adversary can intercept exchanged information within the IoMT edge network through eavesdropping, by tracking communications and reading the contents of the transmitted packages.[21] The adversary can passively intercept the communication between a wearable sensor, which wirelessly transmits patient's vitals to an IoMT gateway (eg, patient's smartphone), and extract confidential data (eg, through traffic analysis) in order to maliciously use them.[42] Moreover, interrogation attacks, which might be considered as a type of impersonation, could compromise data confidentiality.[20] More precisely, a malicious actor might pretend to be a legitimate entity, sending requests in other entities, with only purpose the exposure of private information about the users.[43]

5.2 Security threats to integrity

A man-in-the-middle (MitM) attack is a kind of attack that can jeopardize the integrity of IoMT edge networks, since the attacker interposes in the communication between the two parties and may modify the exchanged data without being noticed.[21] For instance, the collected medical data of the IoMT edge network can be transmitted to a remote server or stored locally in the internal memory of the wearable devices. In case of transmission, a MitM attacker can intercept and modify the transmitted medical data compromising their integrity.[22, 44, 45] Furthermore, the authors in Reference 22 refer to the malicious node injection attack as the most dangerous physical attack since it is not only interrupting the provided services but also modifying the stored data.

Moreover, common attack types targeting to blunt the integrity of IoMT devices successfully include the physical attacks on the devices themselves.[20] For instance, an adversary, who has physical access to an IoMT device, may change its structure so as to alter its behavior. Finally, the lack of lightweight malware detection mechanisms for IoMT devices allows attackers to compromise medical devices' integrity as well.[20] For instance, an attacker can harm an IoMT device by executing a malicious code on it in and exploiting its security holes in networking software and hardware.

5.3 Security threats to authentication

Authentication is one of the essential security requirements of an IoMT-based healthcare system. Because of the ubiquitous characteristics of the IoMT devices, the traditional PKI-based authentication solutions are inefficient and nonexpandable.[46] Moreover, adversaries aim at the poor authentication of a system in order to gain access to resources based on users' identity, without having genuine credentials.[47]

The most common attacks directed at the authentication process are presented in References 45, 47-50. In forgery attacks, the first part of the attack aims at the counterfeit construction of identity, so that the malicious user can be authenticated. Afterward, the attacker transmits fake data in order to defraud other entities.[48]

Furthermore, sybil attacks, where an IoMT device claims multiple fake identities, can be harmful by allowing rogue devices to impersonate other legitimate devices within the IoMT edge network. For instance, the rogue node can achieve to connect with several other IoMT devices in order to maximize its influence and even deceive the system to draw incorrect conclusions.[50] In Reference 51, a taxonomy of sybil attacks in sensor networks is presented, where the attacks are categorized in three different categories: (i) communication of nodes, (ii) identity origin, and (iii) simultaneity. More precisely, the first category is distinguished in direct and indirect communication, characterized by the possibility of “sybil

devices" to communicate directly with legitimate devices or through a malicious device, respectively. The second category is analyzed in fabricated identities, where the adversary could pick random identities for the rogue devices, or stolen identities, when the malicious actor cannot insert new fake identities of devices in the system, resulting in stealing already existing legitimate identities. Finally, the third category is distinguished by the synchronous or asynchronous connection of sybil identities. An attacker might have the ability and the physical equipment to connect with multiple fake identities at once or he or she might choose to participate with a small number of sybil identities at a time, because of hardware or power constraints.

Unlike sybil attacks, in device cloning/replication attack, each device has only one identity. In this type of attack, an adversary takes over a sensor device and extracts encrypted information, which is used in order to create a significant number of clones in the network and perform other attacks, compromising authentication and security objectives.[52] This malicious action is succeeded when the authentication process does not include location-based schemes, in order to banish devices located in the exact same location.[51]

Finally, masquerading attacks may target IoMT edge networks as well. A masquerading attack can fall into one of the following two categories: either an adversary pretends to be a legitimate user in order to gain access to services that IoMT devices provide, via the insertion of rogue devices,[20] or an attacker is allegedly presented as an IoMT device in order to offer fake services to users. The last case is hazardous in the healthcare sector, where the services provided by the IoMT devices are life-dependent for a number of patients.[48]

5.4 Security threats to authorization

Adversaries may target poor authorization mechanisms of an IoMT edge network to achieve access to network resources without having the appropriate access rights. According to Reference 20, due to user's lack of security training and awareness, IoMT devices may be vulnerable to social engineering attack and thus, a malicious actor may trick the IoMT edge network and impersonate as legitimate in order to get access to user's medical devices. Regarding medical devices that oversee vital signs, this may endanger patient's life.[53]

In addition, malware attacks may also compromise the connected IoMT devices by exploiting their inherent vulnerabilities, for example, weaknesses in authorization mechanisms. The infected IoMT devices can be used as bots to launch further attacks on other devices within the IoMT edge network and thus, the attacker can obtain access to the network services (eg, control of several IoMT device) or resources (eg, the collected medical data of a patient).[20]

5.5 Security threats to availability

IoT technology is increasingly used in healthcare applications in order to overpower the disadvantages and limitations of the existing centralized cloud-based healthcare systems. However, the healthcare systems, where the existence of IoMT devices is dominant, are facing the constraints in resources and computational power,[54] raising challenges in preserving the availability of the services provided. In fact, IoMT edge network can become very vulnerable to denial-of-service (DoS) attacks due its constrained resources. Various types of DoS attacks can be applied to different network layers and affect differently the IoMT edge network, such as tampering attacks, jamming attacks, battery drainage attacks, collision attack, congestion, and IoT-botnet attacks.[55]

More precisely, tampering is referred to as the alteration of transmitted data in such a way that IoMT edge network's operations are disrupted. In IoMT edge network environment, the hard detection of a tampering attack is due to the nature of poor and unsecure wireless connectivity.[48] Moreover, jamming attacks are based on the enormous size of transmitted messages in order to overload the communication channels or the computing resources, so that IoMT devices are prevented from using the services provided normally.[48] Jeopardizing the availability of an IoMT edge network, makes it immediately useless in providing real-time healthcare services and may endanger patient's health. For instance, in an IoMT-enabled healthcare alert system, if the communication channels within the IoMT edge network are jammed, the patient in critical condition may not receive the care he/she needs, and thus his/her lives may be at risk. The same result might be caused due to a battery drainage attack against an IoMT device that aims at the battery consumption of the resource-constrained IoMT device.[56] A battery drainage attack can be achieved by an adversary who maliciously sends fake or false messages to the target IoMT device.[57]

Furthermore, in collision attacks, two nodes simultaneously transmit data on the same frequency channel, resulting in identification mismatch at the receiving end. This causes discard of the corrupted received data packets and retransmission of the same packets leading to waste of network resources within the IoMT edge network.[58] In addition, channel congestion attack is achieved through the massive transmission of useless messages, causing high traffic in channels and making time-related IoMT services and data unavailable.[58, 59]

Finally, distributed denial of service attacks can also target the availability of the IoMT edge networks, where an attacker, through an IoT botnet, can flood the target device (eg, gateway) with multiple requests in order to overload them and disrupt the provided services. It is worthwhile to mention that the IoMT edge network is more vulnerable to DoS attacks compared with the Cloud platform in a IoMT-based healthcare system, because of the constrained resources of its devices.[48]

6 SECURITY COUNTERMEASURES IN IoMT EDGE NETWORK

In this section, we present a categorization of security countermeasures, derived from the literature, against the aforementioned threats to IoMT edge networks. The studied countermeasures are categorized based on the security objectives that they ensure within IoMT edge networks.

6.1 Ensuring confidentiality

Within the IoMT edge network environment, special care must be given to the management of data generated, stored, transmitted, and processed by the IoMT devices which are considered confidential. In order to protect data confidentiality in resource-restricted IoMT devices, lightweight encryption protocols have been introduced by following the specifications presented in ISO/IEC 29192.[60] There is a great amount of lightweight cryptographic schemes, such as symmetric key ciphers (ie, block and stream ciphers) and hash functions, which can establish secure communication between constrained IoMT devices, such as the medical sensors and nodes.[48] Nevertheless, symmetric key ciphers suffer from the key distribution problem. For instance, fixed preconfigured keys in IoMT devices are vulnerable to compromise. Moreover, secret keys should be updated automatically, since many users, for example, elderly people are unable or unwilling to configure secure secret keys or update them frequently. In principle, shared keys should be generated with high agreement between the two communicating entities, high randomness, at a first rate, and with a minimum computational/energy overhead.[48] Consequently, the generation of shared keys comprises a challenge for IoMT devices and several works have already been proposed to deal with it. Although symmetric key cryptography is more lightweight, ensuring privacy preservation for the resource-constrained IoMT devices, there are still open issues in meeting the public key cryptography's requirements with the limitations of IoMT devices.[61-63] For example, the level of complexity of the certificate path processing in a healthcare PKI infrastructure is one factor that affects the efficient adoption of PKI technology in healthcare networks.[63]

6.2 Ensuring integrity

In Reference 64, the authors present a combination of symmetric cryptography and attribute-based encryption (ABE) in order to ensure the integrity of the transmitted data in the IoMT edge network environment. The transmitted messages are encrypted with a random symmetric key (RSK) which is encrypted with ABE. If an IoMT device has the correct secret key that satisfies the ABE access policy, then the RSK and the message are decrypted. The secret key is tagged with the device attributes set which represents the user's privileges. In this case, by legitimately changing the system configuration, there is the option of encrypting

the downloaded RSK, instead of the entire message, gaining in communication extent and encryption cost.

On the other hand, another mechanism is elliptic curve cryptography (ECC), which is used as a more lightweight, in terms of computational cost, cryptographic scheme for encrypting the public key, using smaller key size compare to the RSA.[65]

It can further be deduced that almost all the communication protocols such as 802.15.4, ZigBee and LoRaWAN provide conventional cryptographic security assurances such as data integrity. However, the cryptographic security embedded in communication protocols is not meant to protect against node compromise and malware attacks.[20, 66]

Accordingly, apart from data integrity, software integrity is being considered a key element to guarantee security and privacy of the IoMT edge network.[20]

6.3 Ensuring non-repudiation

When disputes come from an entity denying previous commitments or actions, a means to resolve this situation is essential. In IoMT devices, a commonly used means to handle these situations is access log where all the performed operations by/on them are stored securely. In other words, auditing ensures nonrepudiation in IoMT edge network environment. However, auditing should be complemented with appropriate mechanisms to detect and block attacks against nonrepudiation as well as with mechanisms (eg, encryption, access control) that will allow the prevention from occurring at first.[67]

6.4 Ensuring authentication

Authentication is a fundamental requirement for the security of IoMT. A great amount of authentication protocols and techniques exist, but the resource constraints of IoMT devices pose one key problem: the combination of heavyweight authentication techniques with their limited battery and computing power.[47] Thus, a lot of effort should put on lightweight authentication mechanisms for IoT networks such as the IoMT edge networks.[48, 49, 54, 68, 69]

For instance, an authentication technique which is recommended in Reference 70 is an improved certificate-based DTLS handshake protocol, with three major changes: (i) prevalidating the certificates at the IoMT nodes in order to reduce the tasks executed in the constrained devices; (ii) forwarding resumptive sessions so as to decongest the transmission and the processing overhead; and (iii) delegating the handshake procedure for devices that cannot execute a certificate-based DTLS handshake, due to resource constraints, to the devices' owners. It is

worth mentioning that with the implementation of these modifications, the use of certificates appears to be less heavyweight.

However, there is still carried out a lot of research about lightweight versions of authentication techniques suitable for IoT devices that can be also applied to IoMT devices. More precisely, in Reference 71, a lightweight mutual authentication scheme is proposed, between wearable or implantable sensors and a server, for wireless body area network. It is based only on hash function operations and XOR operations without using asymmetric key encryption. In this scheme, there is an access point, which acts as a gateway between the IoMT device and the server, forwarding messages to and from the IoMT device. According to Reference 71, the communication cost and computational time of the proposed scheme are similar to other lightweight authentication schemes,[72, 73] but it is considered more secure against multiple type of attacks in IoMT edge networks such as eavesdropping, jamming, spoofing, replay attacks.

Moreover, in Reference 74, the authors present an one time password (OTP) authentication scheme for IoT, based on asymmetric key encryption, using identity-based ECC and Lamport's OTP algorithm. The proposed scheme is using a private key generator with smaller key size, which is resulting in a lightweight version, suitable for constrained devices such as the IoMT devices.

Furthermore, another mechanism for mutual authentication between an IoT device and a server that can also be applied to IoMT edge networks is given in Reference 75. The proposed mechanism is based on challenge-response mechanisms using physical unclonable functions that are unique, noninheritable, and nonreproducible physical characteristics of the IoT devices, just like fingerprints for the human beings. In particular, in this scheme, challenge-response pairs are formed using the time-based one-time password algorithm mechanism. The presented protocol's key feature is the lack of secret information (ie, secret keys) that is stored in the IoT devices, which keeps the storage overhead very low. Based on the performance evaluation results described in Reference 75, the authors conclude that the proposed mechanism is not only secure against attacks to authentication, but also suitable for real-time applications, such as healthcare services provided by resource-constrained IoMT devices, because of their low computational and communication overhead.

Besides, in Reference 76, a lightweight, privacy-preserving authentication, and key agreement protocol, named PPAKA-HMAC and an improved protocol, named PPAKA-IBS are examined. The first one combines group key agreement with hash-based message authentication code (HMAC) and pseudonym management for secure communications between the devices, and the second one uses identity-based signature (IBS) by contrast to PPAKA-HMAC. The first one ensures secure communication and security against external malicious actors through a lightweight manner, but the second one provides resistance in internal malicious

actions. Both are thought to be suitable for mutual authentication of IoMT devices for real-time IoMT edge networks.

In addition, the authors in Reference 77 present a mutual authentication scheme for a proposed secure IoT-based healthcare system using body sensor network (BSN) and called BSN-Care. More specifically, in BSN-Care system, sensors are connected to a local process unit (LPU) which sends and receives data to and from a BSN-Care server. A lightweight anonymous authentication protocol is proposed, which can be applied to the verification process between the LPU and the server and also between the sensor nodes and the LPU.

Concluding, it is worthwhile to mention that although a great number of authentication schemes for IoT devices have been proposed by researchers, a lot of effort should be put in the future in the design and development of authentication mechanisms suitable for the resource-constrained IoMT devices.

6.5 Ensuring authorization

In principle, access control has been proven to be a reliable tool to ensure the authorization objective. In the case of the IoMT edge network, access control mechanisms may provide restricted access to the IoMT devices according to the requester's privileges where access control information is specified. Consequently, the level of access for each authorized requester can be controlled and thus reducing the risk of intrusion attacks. It is noteworthy to say that access control is also a method to achieve data confidentiality for the stored data on the IoMT devices.[67] A good example of access control mechanisms is the access control lists (ACLs) which constitute an implementation of discretionary access control models based on the access matrix. The ACLs define the operations or data that an authenticated requester is authorized to execute or access, respectively. It is worthwhile to mention that such permissions are permanent once the ACLs are programmed.[67]

In Reference 68, the authors proposed a meta fog-redirection with grouping and choosing (GC) architecture to monitor patient's health status on a pervasive and ubiquitous basis through sensors on the body area network. Regarding this framework, GC architecture with key management scheme and data categorization function regarding the significance of the data (sensitive, critical, and normal) ensures that only authorized entities can obtain access to certain resources in IoT.

Despite the efforts on access control mechanisms for ensuring authorization in IoT-based systems, there are still many open issues to address in order to develop robust access control mechanisms for heterogeneous resources in IoMT edge network environments.[78]

6.6 Ensuring availability

Considering the criticality of the data in an IoMT edge network environment, the availability of the interconnected medical devices should be ensured. IoMT devices face limitations, as mentioned above, on resource and computational power.[54]

Concerning jamming attacks, several research works have been focused on fully or partially centralized schemes and solutions.[79-81] In addition, in Reference 82, a trigger identification service for defending reactive jammers is introduced. According to this scheme, nodes, whose transmission behavior is close to the jamming nodes' behavior, are identified and distinguished. Although, this scheme could successfully demolish the malicious actions, all the decisions made are cloud- or server-based. In addition, the use of algorithms based on pattern recognition of the nodes' transmissions is a very promising solution, but the use of a centralized system is imperative in order to meet the computational cost.[49]

In addition, strength of crowd (SOC) protocol is distributed and might be suitable for resource constrained IoMT devices. This protocol guarantees the delivery of messages to the receiving nodes, although a large proportion of the available bandwidth may be blocked. Specifically, SoC relies on deceiving the adversary, transmitting deception packets from legitimate devices to the network, confusing the jammer on which are the real ones.[83]

Another type of attacks that need to be treated, in terms of availability, with particular care is the DoS attacks. Given the lightweight and low computational nature of IoMT devices, adversaries may manipulate them in order to overflood the communications and services of the edge network with a large number of request messages that may also result in the battery drain of the devices.[84] A solution could be the adoption of a lightweight pattern/behavior recognition algorithm combined with a notification system, in order to detect abnormal activities.[85]

It is worth mentioning that further research should be made in order to mitigate the threats that compromise the availability of the critical services provided by an IoMT edge network environment, moving toward the edge of the network and aiming at addressing the challenges due to the IoMT devices' constraints.

7 CONCLUSIONS

IoMT edge networks aim to improve the patient's quality of life by enabling ubiquitous and personalized healthcare services such as a private healthcare provider round the clock. However, IoMT edge networks are vulnerable to various types of security threats and thus, they may pose a significant risk to patient's privacy and safety. Based on that and the fact that security is a critical factor highly dependent on the reliability of the involved IoMT devices, for the successful deployment of IoMT technology into pervasive healthcare systems, there is an urgent need for novel security mechanisms to preserve the security of the IoMT edge networks. Therefore, we first provided a categorization of existing and

potential threats to the IoMT edge network environment based on the following major security objectives that these threats target: confidentiality, integrity, nonrepudiation, authentication, authorization, and availability. In addition, we provided a categorization of security countermeasures, derived from the literature, against threats to IoMT edge networks. The objective of this work is twofold: (i) to give researchers a better understanding of the threats to the IoMT edge networks and the countermeasures against these threats, and (ii) to provide a foundation for organizing research efforts toward the design and development of proper lightweight security mechanisms overpowering the limitations of the IoMT devices, in terms of resources and computational power, and preserving the security in IoMT edge networks.

REFERENCES