Future Generation Computer Systems 105 (2020) 581–606

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Securing internet of medical things systems: Limitations, issues and recommendations

Jean-Paul A. Yaacoub [a,b], Mohamad Noura [c], Hassan N. Noura [a,b], Ola Salman [a], Elias Yaacoub [d], Raphaël Couturier [c,*], Ali Chehab [a]

[a] American University of Beirut, Electrical And Computer Engineering, Lebanon
[b] Arab Open University, Department of Computer Sciences, Beirut, Lebanon
[c] Univ. Bourgogne Franche-Comté (UBFC), CNRS, FEMTO-ST Institute, France
[d] Computer Science and Engineering Department, Qatar University, Doha, Qatar

ARTICLE INFO

Article history:
Received 2 March 2019
Received in revised form 18 November 2019
Accepted 18 December 2019
Available online 24 December 2019

Keywords:
Healthcare
IoMT
Medical cyber physical systems
Medical devices

ABSTRACT

Traditional health-care systems suffer from new challenges associated with the constant increase in the number of patients. In order to address this issue, and to increase the accuracy, reliability, efficiency, and effectiveness of the health-care domain, the Internet of Medical Things (IoMT) was proposed. IoMT can be considered as an enhancement and investment to respond more effectively and efficiently to patients' needs. However, IoMT suffers from different issues and challenges such as the lack of security and privacy measures, in addition to the necessary training and awareness. In this paper, we highlight the importance of implementing the right security measures and the required training skills, in order to enhance the immunity of IoMT against cyber-attacks. Moreover, we review the main IoMT security and privacy issues, and the existing security solutions. These solutions are classified as cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity and required resources. It is important to note that the security measures for IoMT exhibit a trade-off between the security level and the system performance, especially in the rise of digital healthcare v4.0 era. Next, we discuss the appropriate security solutions such as lightweight cryptographic algorithms, and protocols that attempt to reduce the overhead in terms of computations and resources. This leads to the conclusion that there is a need to design an efficient intrusion detection/prevention system that cooperates with dynamic shadow honeypots. Finally, we propose a security solution, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patients' privacy. However, it should be noted that zero-day attacks and exploits are still the main challenging issue that surrounds IoMT.

1. Introduction

The integration of medical devices within the Internet of Things (IoT) (see Fig. 1), led to the emergence of the Internet of Medical Things (IoMT) [1]. With the emergence of the new digitized healthcare era, called Healthcare v4.0 [2,3], IoT devices were deployed in several medical domains, especially with the excessive use of medical wireless sensors, devices, Unmanned Aeria Vehicles (UAVs), and robots. In fact, medical sensors and actuators are used as wearable devices in the context of body area networks. Instead of keeping patients in hospitals, these devices are capable of constantly monitoring the patient's health in real-time, while offering them better physical flexibility and mobility. On the other hand, medical robots can also serve as surgical robots, as well as hospital robots [4], which are capable of accurately performing small surgeries. They are also capable of performing several medical tasks such as Cardio-Pulmonary Resuscitation (CPR) [5]. However, the main issue is that many IoMT devices are prone and vulnerable to cyber-attacks simply because medical devices are either poorly secured against potential adversaries, or not secure at all. Therefore, any cyber-attack can have drastic consequences, threatening patients' lives, which would hinder the wider deployment of IoMT.

Furthermore, IoMT applications are closely related to sensitive healthcare services, especially that they handle sensitive information about patients including their names, addresses, and health conditions. The main challenge in the IoMT domain is preserving

[*] Corresponding author.
E-mail addresses: jp.jacob1@hotmail.com (J.-P.A. Yaacoub), mohamad.noura@univ-fcomte.fr (M. Noura), hn49@aub.edu.lb (H.N. Noura), oms15@mail.aub.edu (O. Salman), eliasy@ieee.org (E. Yaacoub), raphael.couturier@univ-fcomte.fr (R. Couturier), chehab@aub.edu.lb (A. Chehab).

https://doi.org/10.1016/j.future.2019.12.028
0167-739X/© 2019 Elsevier B.V. All rights reserved.

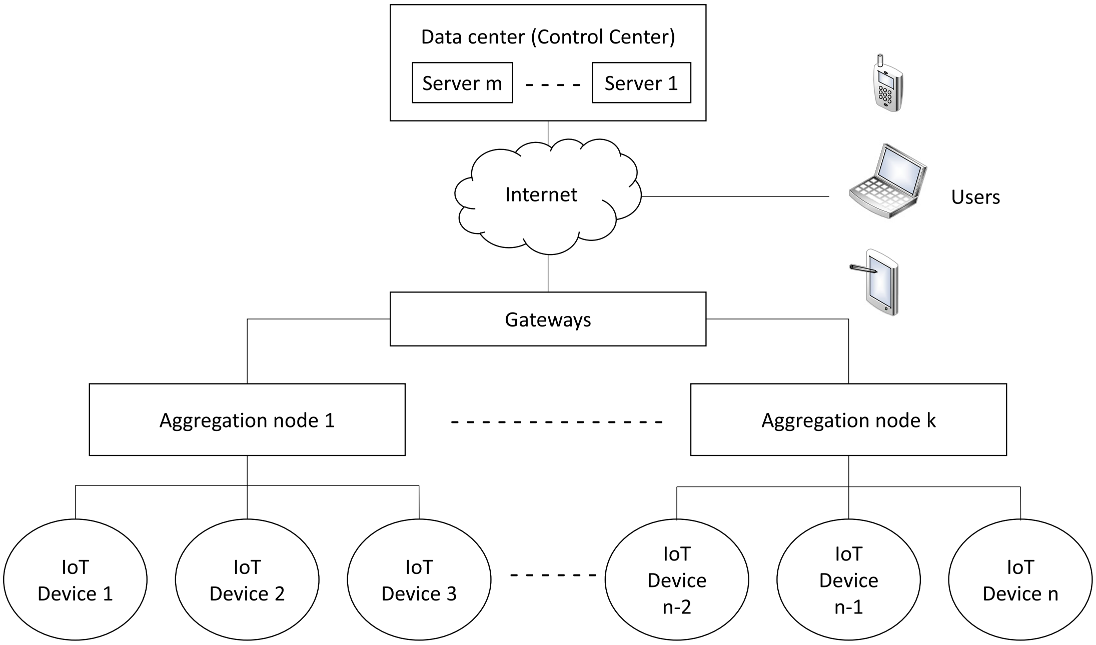

Fig. 1. An example of Internet-of-Things system with n IoT devices, k aggregation nodes & m servers.

the patient's privacy without degrading the security level. In addition, appropriate security and privacy solutions should include minimum computations and require minimal resources.

1.1. Motivations & aims

Recently, medical IoT systems became among the most important advanced medical technologies. This technology can achieve a significant gain by enhancing the remote monitoring of medical services. Moreover, it can help in detecting any medical issue very early and thus, preserve patients' lives and health.

However, in the IoMT domain, many of the connected medical devices present security vulnerabilities that make them prone to malicious exploitation attempts. Such issues may lead to drastic consequences, which would affect patients' lives by perturbing (or controlling) medical devices. Therefore, it is mandatory to overcome these issues to preserve the efficiency and accuracy levels of medical IoT systems.

On the other hand, the pervasiveness of medical sensitive data within IoMT systems makes them prone to advanced attacks (e.g. Ransomware) that target their main security aspects including privacy, integrity and confidentiality. This would severely impact the credibility, adoption, and wide deployment of IoMT systems.

Our aim, in this paper, is to identify the main threats that may compromise the security of IoMT devices and systems, and to identify the necessary and appropriate measures that are essential for their security.

1.2. Related work

Medical IoT systems became core to the e-Healthcare domain whereby smart medical sensors and devices are installed to improve patients' lifespan and medical conditions. However, this domain came under a variety of attacks such as botnets targeting medical systems [6], as part of targeted cyber-crimes [7]. In [8], IoT security and privacy issues were discussed but were not effectively linked to IoMT. Various intrusion detection [9,10] and authentication/authorization [11,12] methods were presented to ensure a secure IoT environment with little notice to their application to IoMT. Moreover, only recently more work was directed to the security of healthcare systems. A generic survey on medical big data analysis was conducted in [13] to sort big data issues and challenges of adopting IoMT solutions [14], while an on-demand IoT adoption in hospitals was conducted in [15] to enhance nurses' experience based on the pros and cons of the IoT adoption in healthcare technologies [16]. In this paper, we present a more detailed, holistic and analytical view point on the IoMT and healthcare domains, as well as the integration of cyber–physical systems within the medical field. All the mentioned cyber-attacks exclusively target healthcare systems, while the presented security measures are discussed in a way to ensure their adoption in such domains.

1.3. Contributions

The novelty of the paper stems from the fact that it includes a comprehensive overview and analysis of all security and privacy issues related to medical IoT systems. Also, the paper discusses the recent lightweight security solutions, which consist of cryptographic and non-cryptographic techniques. Moreover, several lessons are learned from the overview and accordingly, several recommendations are proposed towards making medical IoT systems secure and safe to deploy and use.

More specifically, the contributions of this paper can be summarized in the following points:

- **Perspective & Future Trends** of IoMT systems are presented, including their communication types, device types, and applications.
- **Benefits** of IoMT systems and applications are presented and discussed.
- **Concerns & Risks** are highlighted, especially in terms of public and privacy concerns, while risks are presented and evaluated through a proposed qualitative risk analysis method.
- **Attack Sources & Characteristics** are presented and discussed in details, including their scope and impacts.

- **Cyber-Attacks** are presented per security breach, while exploring malware and code injection attacks. Moreover, real-case cyber-attacks are also presented.
- **Security Measures** including technical and non-technical ones are presented, evaluated and analyzed especially in terms of their advantages and limitations.
- **Suggestions & Recommendations** are presented based on the conducted research for a much more efficient and secure IoMT environment.

1.4. Organization

This paper is divided into seven sections, in addition to the introduction, which sheds light on the digitization era of healthcare v4.0. Section 2 presents and details the main IoMT communication protocols and application domains. Section 3 highlights the main IoMT challenges, constraints, concerns, and risks, while presenting a qualitative risk assessment. Section 4 presents and discusses the most recurring cyber-attack types against IoMT main security goals, including real-case cyber-attacks against well-known hospitals in the United Stated (US) and the United Kingdom (UK). Section 5 presents various technical and non-technical security measures that are suitable for protecting the IoMT and e-Healthcare systems, communication and devices, along with their advantages and limitations. Section 6 highlights this paper's main suggestions & recommendations which include the adoption of lightweight cryptographic solutions, hybrid and dynamic non-cryptographic solutions, and finally the implementation of artificial intelligence for a higher accuracy and in a real-time. Section 7 concludes the presented work with some prospects on future work.

2. IoMT background, perspective & future

In this section, the main communication types used in IoMT are presented, in addition to the different types of medical devices, as well as the benefits offered by IoMT systems. Moreover, the future prospects of IoMT are also highlighted and presented in Fig. 2.

2.1. IoMT communications

Real-time data transmission among medical devices takes place via four main communication networks types. These types include Body Area Networks, Home Area Networks, Neighborhood Area Networks, and Wide Area Networks.

- **Body Area Network:** A Body Area Network (BAN) is a network medium for the transmission of patients' vital signals, which are measured by either a wearable or a portable sensor. In [17], Kocabas et al. stated that the communications between medical devices can be secured using biomedical signals. Therefore in [18], Poon et al. presented a low-power bio-identification mechanism by using an Inter-Pulse Interval (IPI) to secure the communication between Body Area Network sensors. In [19], Venkatasubramanian et al. managed to use a physiological signal that agrees over a secret key of the symmetric key cryptosystem for BAN sensor communications. As a result, the collected medical data is sent to the controller in two different ways:
  - **Smart-Phone:** transmits the collected data via a mobile network to the base station (BS) that routes it until it reaches the medical data center.
  - **Wireless Medical Device:** (see Fig. 3) transmits data using one of several wireless communication protocols such as Zigbee [20], Bluetooth [21], or Wi-Fi [22].
- **Home Area Network:** A Home Area Network (HAN) uses a controller, which handles the communication for sending the gathered data to an available Access Point (AP) located in the patient's home. Transmissions can rely on Wi-Fi, or LTE/LTE-A [23] in case of a Femtocell AP [24].
- **Neighborhood Area Network:** A Neighborhood Area Network (NAN) enables users to quickly connect to the Internet [25]. It is used to establish wireless communication between close areas such as homes and their neighborhoods. It can be based on an omnidirectional antenna that allows a single AP to cover a radius of at least half a mile. Moreover, a NAN can rely on a directional antenna to improve the AP's signal as shown in Fig. 4. As such, the AP forwards the data to a mobile data station, which allows the data sent from the home's AP to be directly received at the mobile Base Station (BS).
- **Wide Area Network:** A Wide Area Network (WAN) represents the communication from a mobile Base Station or from an access point to the mobile/Internet (remote) medical infrastructure. In case of emergencies, a WAN ensures real-time data transmission to emergency response teams. Once the data is received, the AP can also send the data to cloud services for storage at the specified server.

2.2. IoMT devices & protocols

Medical devices are differentiated according to their needs. In fact, many of them are available as a gadget in the medical market, or are being used by hospitals for real-time smart remote monitoring. These smart medical devices can range from fitness devices, to blood-pressure devices, to sugar-level devices. A set of these medical devices is listed in Table 2.

Given that the aging population in developed countries is growing, there is a need for a much more sophisticated and suitable health-care system. The recent IoMT technology is considered as one of the most important solutions, which was introduced to answer the growing needs and demands. IoMT ensures physical mobility for patients, which leads to the reduction of the number of patients in a hospital performing Blood Pressure (BP) tests, or a Cardio-Vascular Disease (CVD) tests, which constitute 30% of global death, as stated by the World Health Organization (WHO). Moreover, diabetic cases can now be remotely monitored from hospitals.

These devices can be either implanted, worn, or held. Moreover, some devices can be used in-home and others are specialized and to be used in hospitals and clinics. In the following, we give examples of such devices. The different protocols supported and employed to (inter-)connect such devices are listed in Table 1.

- **Wearable and Personal Devices:** these include smart and electronic medical devices that collect, monitor and improve patients' health conditions in a real-time manner, and at a reduced cost [26]. Wearable devices include fitness trackers, smart health watches, wearable Blood Pressure Monitors (BPM), ring-type heart rate monitor and biosensors [27,28]. Due to the increase in the number of aging population and spread of diseases, there is even a higher demand for tele-home healthcare. In the following some of these devices are described in detail.
  - **Smart Fitness Devices** are used to maintain a healthy lifestyle for patients and to improve their health conditions. This is achieved by adopting a daily workout routine, which varies and depends on the patients' ability and physical status, along with their condition, age and gender. Several additional smart fitness

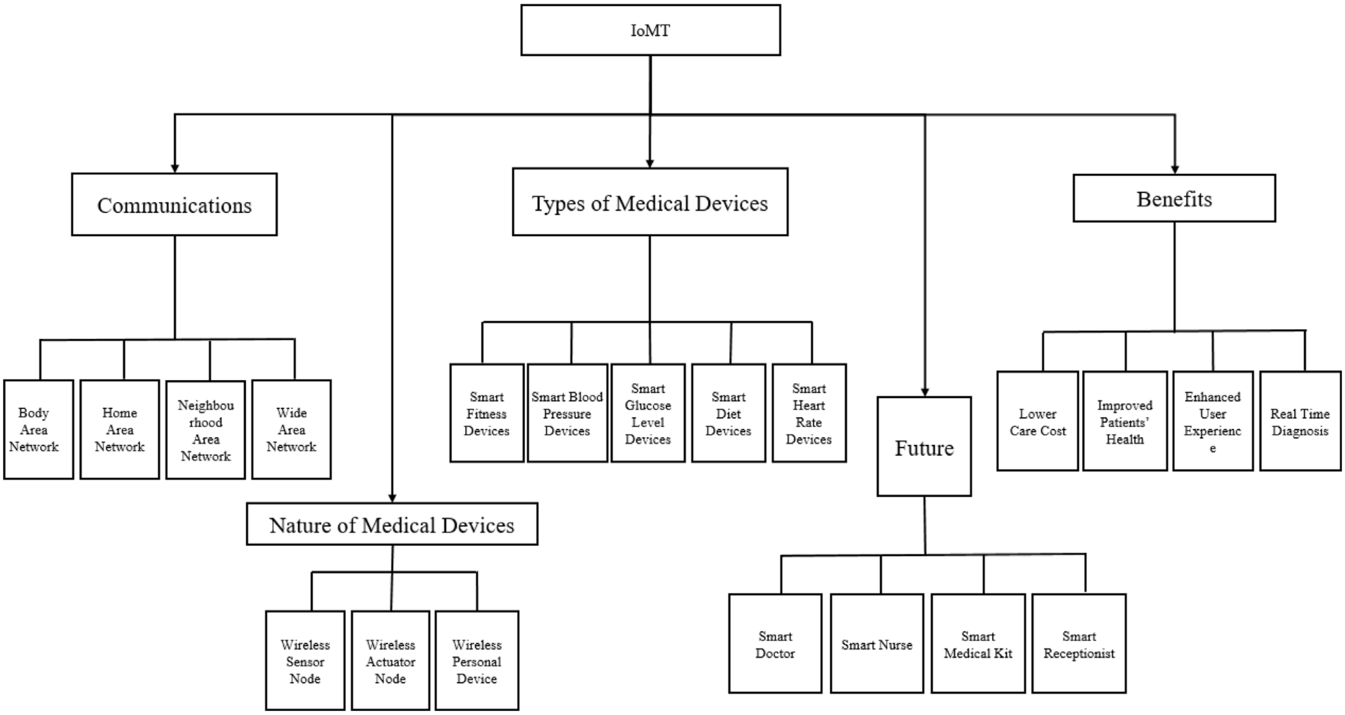

Fig. 2. IoMT's communication, perspective & future taxonomy.

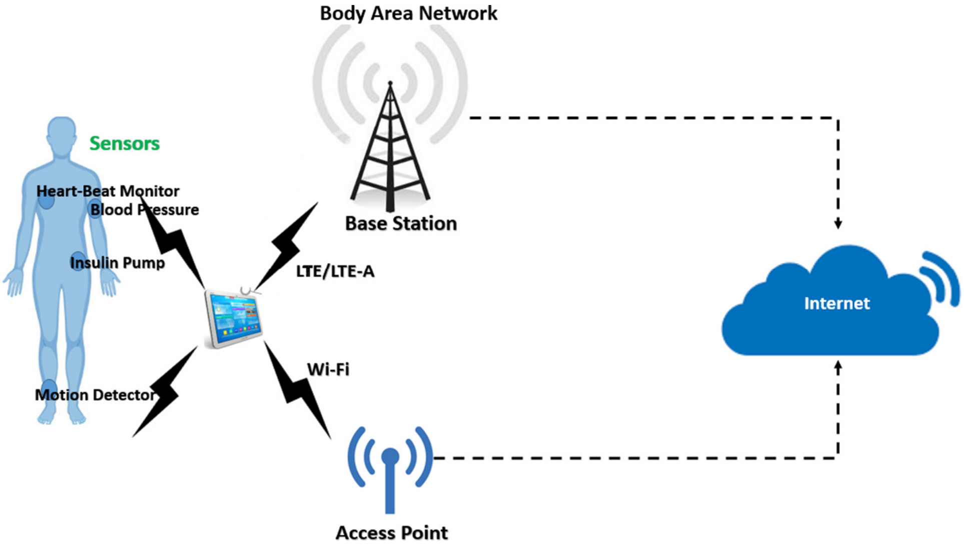

Fig. 3. Body area network.

Table 1
A set of protocols used for IoMT interconnection.

Protocol	Classification	Range	Description
4G or LTE	Wireless	Medium Range	Cellular Technologies that Connects Medical Personal and Wearable Devices
Wi-Fi, 802.1x	Wireless	Medium Range	Reliable, Real-Time, High Power and Long Range Medical Connection
Zigbee	Wireless	Medium Range	Used for Low Data Rate Medical Connections with Minimum Latency & Energy Consumption
Z-Wave	Wireless	Medium Range	Used for Low Data Rate Medical Connections, include Sending Alerts & Tele-Home Healthcare (Remote Monitoring)
Bluetooth	Wireless	Short Range	Used for Short Range Connection to a Nearby Medical Device including Smart Medical Sensors
6LoWPan	Wireless	Medium Range	Used for Medical Low Power Wireless Personal Area Networks
Machine-to-Machine (M2M)	Wireless	Long Range	Real-Time Remote Patient Monitoring & Error Detection, Enhanced Patient Care & Attention
Internet Protocol (IP)	Wireless	Long Range	Software Responsible of IoMT and E-Healthcare Communications

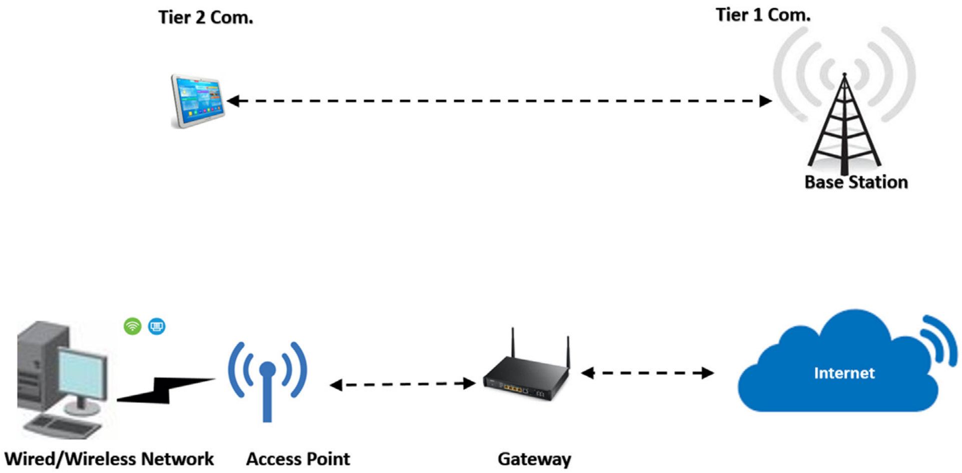

Fig. 4. Neighboring area network.

devices were mentioned in [29], including "TomTom Spark 3", which is a fitness tracker and "on-wrist navigator" [30] and "Moov Now", which is also a fitness tracker [31].

- **Smart Blood-Pressure Devices** are deployed in many IoMT fields and domains. They are used to remotely and continuously monitor the blood pressure of patients. These devices check for deviations in blood pressure from the norm towards detecting rapidly any anomaly and transmitting the data in real-time. A set of such devices includes "Omron EVOLV" [32], "iHealth Feel & View BPM" [33] and "Philips Upper Arm BPM" [34].
- **Smart Glucose-Level Devices** are used to monitor and to track the real-time sugar levels of patients who suffer from diabetes types I and II. They help in maintaining the right insulin level to protect the patients. This reduces the implications and risks associated with unexpected higher or lower levels of insulin. Examples of such devices include the GlucoWise device [35], in addition to turning a given IoT device (mainly smartphones) into a blood sugar meter sensor [36], and iBGStar Blood Glucose Meter [37]. In case of an insulin drop, signals are sent to the actuators of the insulin pump to inject the appropriate insulin dose. Another actuator example is the spinal cord stimulator, which is implanted in the patient's body to ensure long-term pain relief [38].
- **Smart Heart-Rate Devices** are used in several medical domains and they are capable of saving patients' lives. A set of k devices can monitor patients' heart rates in real-time, while other devices communicate only urgent data, when an anomaly is detected. As such, the main task of these devices is to predict any possible heart-attack before it occurs. These devices may include wearable wireless sensor networks and BANs [39], along with different heart-rate monitoring devices [40].
- **Smart Diet Devices** are being used to maintain a healthy diet for patients who mainly suffer from eating disorders. They are specifically used by obese people who struggle in following a certain diet or sometimes forget about diet restrictions. In fact, smart diet devices have become a substitute for paper-written diets. Such devices would send users automatic updates about their daily diets, with different nutrition ingredients, via a smart diet software [41].

- **In-home Medical Devices:** these include ventilators, infusion pumps, and dialysis machines that are currently being used outside the hospital or clinic, which are also provided by a health care professional, and rely on simple technologies (e-mail, the Internet, smart medical devices) to communicate with the hospital [42]. Among these devices, we mention test kits, first aid equipment, durable medical equipment, feeding equipment, voiding equipment, treatment equipment, respiratory equipment, infant care, and other equipment which are further discussed in [43].
- **In-Hospitals and Clinics Medical Devices:** hospitals must always be prepared for any emergency or incidence, whether or not these are life threatening. As such, a high level of readiness of both medical equipment and staff is a must to offer the right treatment for patients. In this context, medical donations play a crucial role [44]. Among such medical devices we list defibrillators, anesthesia machines, patient monitors, Electrocardiogram (EKG) Machines [45], surgical tables, blanket and fluid warmers, electro-surgical units, surgical tables and lights, which are further discussed in [46].

2.3. IoMT application domains

Despite the challenges that surround the IoMT domain, this technology offers several advantages via health-care applications [50]. First, and since the vital signs of a patient could be monitored in real-time, this allows patients and the medical staff to communicate instantly. This reduces the cost of medical care by reducing the number of doctor visits. Improving patients health and lifestyle is another benefit of IoMT. The immediate access to a patient vital signs allows the early diagnosis, the prescription of medication and the injection of medication via a wearable device.

The future of IoMT aims at further involving devices and applications in the roles of doctors, nurses, medical kits and receptionists. However, the general public still has concerns about the necessary security, privacy, trust and accuracy of such IoMT systems.

- **Smart-Doctor:** One of the future plans is to introduce the concept of smart-medical robots to perform the role and tasks of a real doctor. Some patients have expressed concerns regarding this matter while others felt more comfortable speaking to a robot doctor about their private medical issues than they would with a real doctor. Despite the opposing views, in the near future, the term smart-doctor will be frequently heard and used.

Table 2
A set of medical IoT applications [47].

Application	Data rate	Bandwidth (Hz)	Accuracy (bits)
ECG (12 leads)	288 kbps	100–1000	12
ECG (6 leads)	71 kbps	100–500	12
EMG	320 kbps	0–10,000	16
EEG (12 leads)	43.2 kbps	0–150	12
Blood saturation	16 bps	0–1	8
Glucose monitoring	1600 bps	0–50	16
Temperature	120 bps	0–1	8
Motion sensor	35 kbps	0–500	12
Cochlear implant	100 kbps	70–350/3500–8500	16 [48]
Artificial retina	50–700 kbps	<10	12 [49]

- **Smart-Nurse:** Smart-medical robots will also be able to perform secondary medical tasks such as taking the role of a nurse. In many cases, they may perform the task of a smart-assistant to a given nurse to facilitate the nurse's tasks. The plan is to rely on robots to perform a secondary or/and supportive medical task, according to the medical conditions and needs.
- **Smart-Medical Technology:** It includes Smart medical equipment and kits that are currently being deployed and used by paramedics to provide immediate help to patients who are in urgent need of medical care and assistance. One example is the use of medical drones to perform such a task [51]. Medical drones were originally introduced to respond to emergencies related to patients suffering from cardiac arrests [52], since these drones are the fastest to arrive at the emergency scene. The drones would be directed to fly to specific destinations, which saves time and as such, saves lives since paramedics might end up stuck in traffic, and may not be able to respond as quickly as needed. This encourages the reliance on smart medical robots [53] to perform surgical operations within a hospital setting. Virtual/Augmented Reality and Artificial-Intelligence (AI)-based medical technologies were also employed for various medical purposes. This includes Virtual-Reality to perform various realistic operations such as simulated training [54], emergency training [55], and Cardio-Pulmonary Resuscitation (CPR) training [56]. AI-based medical technologies are also being used to ensure a higher accuracy rate [57]. This includes exploring bio-chemical interactions [58], such as IBM Watson and Gene Network Sciences (GNS) Healthcare AI systems [59] used to search for the right cancer treatment [60].
- **Smart-Receptionist:** A smart-receptionist is yet another trend in the IoMT domain; a medical robot is capable of operating as a normal receptionist, having the ability to "think" and "understand" a given medical, or urgent case before diverting the patient towards the right medical department. Also, these robots would answer phone calls and book appointments for patients, whilst classifying the urgent and normal appointments. Such a classification could be based on statistical or machine-learning algorithms.
- **Personal Emergency Response Systems (PERS):** these are seeing increasing use to alert patients and doctors in a real-time manner of any patient's abnormal medical event (E.g stroke, cardiac arrest, seizure etc.) by remotely sending vital signals to the hospital [61] based on a predictive risk assessment method [62]. PERS are now being modified to become location-based [63] for a higher accuracy and faster response time. A typical example is the Active-Protective's smart belt which can be placed on a patient's waist and uses Bluetooth and AI to transmit real-time data.
- **Ingestible Cameras:** these are cutting-edge and cost-effective capsules that can be swallowed (in-vivo/in-vitro) by a patient to provide internal-organ real-time visual monitoring for early detection of chronic diseases and cancer [64]. Many ingestible devices were presented including Swallow-able data recorder capsule medical device [65], ingestible endoscopic optical scanning device [66], and ingestible hydrogel device [67]. Ingestible devices rely on an X-ray or camera capsule, a tracking/recording system and the diagnostics toolkit for evaluation.
- **Real-Time Patient Monitoring (RTPM):** this is a new evolving trend among the new generation, including millennials, due to their heavy reliance on smart devices as a key part of their daily lives [68]. In fact, RTPM is used to ensure a real-time, cost-effective remote consistent monitoring depending on the sensors linked to the patient's body, either through a homecare telehealth systems [69,70] or telecare monitoring systems [71,72]. This may include monitoring fitness level, glucose level, respiration rate, and heart rate, etc. Many new RTPM trends are now available including, but not limited to, connected inhaler delivery systems, Apple Watch app that monitors depression, Apple's Research Kit and Parkinson's Disease and ADAMM intelligence Asthma Monitoring [73,74].

As listed above, IoMT will enable innovative healthcare applications; however, there are many challenges that might hinder the evolution of this technology. One of the key challenges is related to the security and privacy issues. In the next section, we discuss the main security concerns, challenges, and risks that might be associated with the deployment of IoMT systems.

3. Concerns, challenges & risks

In this section, we highlight the main concerns that are related to IoT systems, in general, with emphasis on medical issues.

3.1. IoMT concerns

IoMT-related concerns can be classified into four key categories, one of them is raised by the general public and is related to the security, privacy, trust and accuracy issues.

- **Security Concerns:** Due to the reliance of IoMT devices on the use of open wireless communications, these devices are prone to various wireless/network attacks. In fact, an attacker can eavesdrop and intercept incoming and outgoing data and information due to the lack of security measures that most IoMT devices either suffer from by design, or due to weak security authentication measures that can be easily bypassed by a skilled attacker. Another security issue is the ability to gain unauthorized access, without being detected, due to the inability to detect and prevent such attacks. This would result into gaining an elevated privilege, injecting malicious codes, or infecting devices with a malware. On the other hand, IoMT devices could be hijacked (as botnets) and used to launch Distributed Denial of Service (DDoS) attacks. In [75], Clark et al. showed how medical devices are prone to botnets or "zombies" attacks, which can lead to physical attacks on human patients. An attack, for example, can logically manipulate a drug dose that would kill or have serious health implications on a given patient. Moreover, IoMT devices, when hijacked by terrorists, could be used as a mean for targeted assassination. For this reason, the US Vice President, Dick Cheney, disabled the wireless functionality of his heart implant out of fear of being hacked to eliminate him [76]. Moreover, as described in [75], IoMT devices can have a negative effect on the psychological state of patients, since these can potentially scare patients, causing them to suffer from a heart-attack due to being surrounded by machines instead of humans.

Manufacturers of medical devices need to focus on security as a primary task to ensure and maintain the security of the Medical-Cyber Physical System (MCPS), along with medical systems and devices alike. In other terms, protection against passive and active attacks is a must to mitigate the main IoMT security concerns. Hence, the need for the right security measures and tools is crucial.

- **Privacy Concerns:** Passive attacks such as traffic analysis leads to privacy issues since it would be possible to gather and disclose information about patients' identity, in addition to sensitive and confidential information.

  This is a very serious threat for patients since an attacker is capable of identifying his/her medical records and medical conditions, which poses drastic life-threatening effects on patients.

  Another reason for breaching the privacy of patients, through attacking hospitals, is identity theft. Most of these real-case attacks led to a breach of patients' privacy either through the leakage, or through the disclosure of personal/sensitive information.

  As a summary, privacy is more than ensuring the secrecy of sensitive and private medical information. It also entails the need for anonymity, non-linkability, and non-observability.

  - **Anonymity:** a patient should not be identifiable; when a patient is in communication, his identity should be kept hidden. In other terms, passive attacks can see what you do, but not who you are.
  - **Non-Linkability:** Items of Interest (IoI) such as subjects, messages, events, actions should not be disclosed by passive attacks. This means that the probability of those items not being exposed from the attacker's perspective should stay the same, before and after observation.
  - **non-Observability:** non-observability is the state of Items Of Interest (IoI) being indistinguishable from any IoI of the same type. This means that messages are not discernible from any random noise(s). In other words, it should not be noticeable whether, a message has been exchanged between a sender/receiver in any relationship.

- **Trust Concerns:** The breach of patients' privacy translates into serious trust issues. Patients are becoming skeptical of the idea of machines taking over the roles of humans (doctors, nurses, and receptionists). As a result, people are more concerned about having a medical robot, or a medical machine, or even a medical device monitoring and controlling their health conditions [77].
- **Accuracy Concerns:** This type of concern has surfaced after more than 144 patients in the U.S. lost their lives [78] due to accidental mistakes related to medical robots' lack of accuracy and diagnosis. This also resulted into having more than 1400 patients being partially or permanently injured, where reports of malfunction revealed that more than 8061 malfunctions have occurred within thirteen years (2000–2013) [79]. Another example is the false diagnosis of some patients as having dementia or Alzheimer. These incidents indicate the lack of accuracy and precision in the operations being led by medical robots, along with the false diagnosis of patients, and wrong medical prescriptions [80].

3.2. IoMT challenges

IoMT challenges emerged as soon as the integration of medical devices into IoT systems started. One major challenge is the lack of standardization. In [81], Hassanalieragh et al. discussed in details the main IoMT challenges. The issue of standardization is essential to having different medical devices operating together, and for vendors to adopt the right security measures to protect them from being hacked. This would lead to higher protection, efficiency, scalability, consistency, and effectiveness. In fact, many of these challenges are mainly related but not limited to various IoMT security constraints (see Fig. 5).

3.3. IoMT risks

The deployment of IoMT systems into the healthcare domain is associated with a number of risks which are listed as follows:

- **Disclosure of Personal Information** can seriously affect patients' medical conditions, as well as hospital's reputation.
- **Data Falsification** can result into having the transmitted data from any medical device altered and modified, which would result into a higher drug dosage or wrong medical description that can lead to further medical complications.
- **Whistle-blowers** are based on unsatisfied or rogue medical employees leaking medical details and information about the hospital or patients by either being bribed, or part of an organized crime activity, risking patients' privacy and lives.
- **Lack of Training** among nurses and doctors can result into risking patients' lives with permanent disabilities or the loss of life.
- **Accuracy** is still a debatable issue and is still responsible for inaccuracies in the medical operations conducted by specialized robots. This can also seriously affect patients' lives and lead to disabilities or fatalities.

Thus, a new risk assessment method is required to quantify the security risks of IoMT attacks, which is a complicated task. Addressing threats in IoMT and analyzing their associated risks is the first step towards identifying the required security solutions to be adopted by IoMT applications and communication protocols. The risk analysis, presented in [82], is based on Threat, Risk, and Vulnerability Analysis (TVRA) methodology [83]. This methodology is based on the likelihood of a given attack, and the attack impact on the system including the system assets and its associated threats. In addition, the threat agent which is trying to break the system is also identified by the TVRA method. Therefore, the outputs of TVRA are measures of the risk of the already identified threats and can be determined based on their estimated value of likelihood and impact on the system. The existing threats can be ranked as either critical, major, or minor, and they are represented in Table 3, depending on their impact on human emotional conditions, which should also be taken into consideration.

In fact, given the above listed concerns, challenges and risks, it is essential to review the possible security attacks and their causes. Thus, in the next section, we give a detailed description of the attack types, causes and effects.

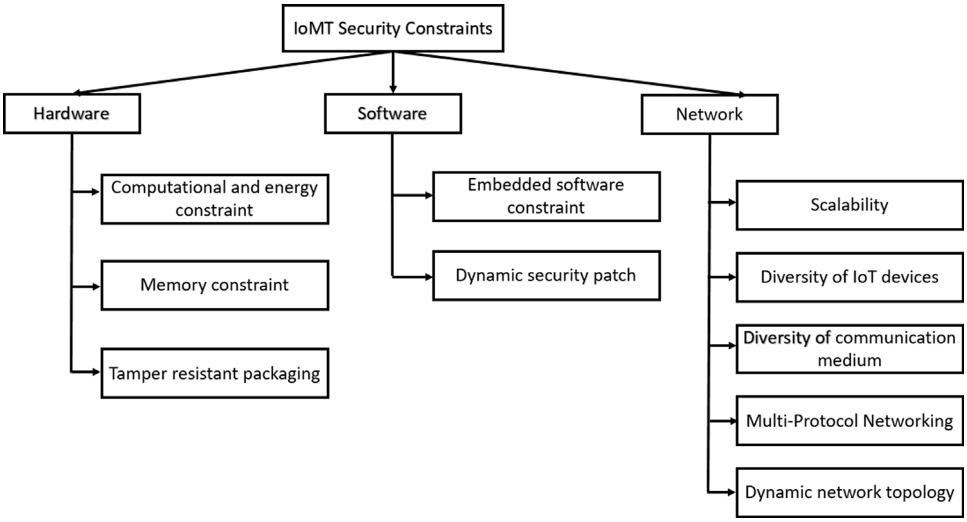
IoMT Security Constraints
Hardware
Software
Network
Computational and energy constraint
Memory constraint
Tamper resistant packaging
Embedded software constraint
Dynamic security patch
Scalability
Diversity of IoT devices
Diversity of communication medium
Multi-Protocol Networking
Dynamic network topology

Fig. 5. IoMT security constraints.

Table 3
Qualitative psycho-emotional medical risk assessment.

Threat	Nature		Motivation		Risk		Emotional/Psychological Impact							
Type	Human	Non-Human	Malicious	Non-Malicious	Likelihood	Impact	Anger	Fear	Mistrust	Sadness	Depression	Anxiety	Guilt	Embarrassment
Medical information disclosure	Yes/No	No/Yes	✓	✕	High	High	Yes	Yes	Yes	Maybe	Maybe	Yes	Maybe	Yes
Medical data manipulation	Yes	No	✓	✕	High	High	Yes	Yes	Yes	No	No	No	Yes	No
Medical data interception	Yes	No	✓	✕	Moderate	High	Yes	Yes	Yes	No	No	Maybe	No	Yes
Medical data hijacking	Yes	No	✓	✕	High	High	Yes	Yes	Yes	No	No	Yes	No	Yes
Medical data exposure	Yes/No	No/Yes	✓/✕	✕/✓	Low/Moderate	Moderate/High	Yes	Yes	Yes	Maybe	Maybe	Yes	No	Yes
Wrong dosage	Yes/No	No/Yes	✓/✕	✕/✓	Low/Moderate	High	Yes	Yes	Yes	Yes	No	Maybe	No	No
Medical data delay	Yes/No	No/Yes	✓/✕	✕/✓	Moderate	Moderate/High	Yes	No	Maybe	No	No	No	No	No
Insiders	Yes	No	✓	✕	High	High	Yes	Yes	Yes	No	No	No	No	Yes
Misconfiguration	Yes/No	No/Yes	✕	✕	Low	Moderate	Maybe	Maybe	Yes	No	No	No	No	Maybe

4. Cyber-attacks against IoMT

Such attacks can either be targeted, organized or even coordinated, based on the attackers' skills, experience, knowledge, and tools in order to carry out a successful cyber-attack. These attacks target the confidentiality, integrity, availability and/or the authentication of a given system and/or its components. In fact, it depends on the malware type used in order to carry out the attack.

4.1. Characteristics of cyber-attacks

Before identifying and classifying a given attack, it is important to understand its characteristics. In general, any attack can be classified as one of five main categories (see Fig. 6), based on its nature, target, scope, capacity, and impact, all of which are directly related to the attacker's purpose, aim, objectives and goals. More precisely, it depends on the attacker's skills, knowledge, experience, available tools and resources at his disposal.

- **Attackers' Nature:** There are four categories of attackers, internal, external, passive and active attackers. In some cases, different types of attackers may collude to ensure a more sophisticated cyber-attack.
  - **Internal & External Attackers:** An ***internal attacker*** is mainly a rogue employee who can be a nurse, a doctor or a medical staff who wants to cause damage to a hospital by damaging its reputation via removing or modifying data, or targeting patients' health and privacy. In some cases, it can be a spy masqueraded as a nurse or a doctor who managed to successfully evade all the security measures of a given hospital to eliminate a given patient for either political or other criminal purposes. Internal attackers might pave the way for external attackers to perform their cyber-attacks easily.
    External attackers are mainly classified as malicious hackers who aim at gaining an elevated unauthorized privileged access into the hospital's system. This is mainly achieved through worms, Rootkits, or Remote Access Trojan attacks. In many cases, the attack is based on spear-phishing techniques through sending a malicious Portable Document Format (PDF) file, or any other file as a Curriculum Vitae (CV). Once downloaded, a backdoor or a key-logger will be installed on the given system. The main aim is to breach the privacy of patients and sell them to malicious third parties through the deep dark web for scamming purposes.
  - **Passive & Active Attackers:** A ***passive attacker*** tries to evade detection by remaining "hidden" in the background, without making any activity. The aim here is to intercept data, transmitted via any wireless communication, between different medical devices, read them and build up their own information gathering process that can be used for further exploitation, which may lead to a much more sophisticated cyber-attack. Passive attackers can be cooperating with external or even internal attackers as part of the information gathering process.
    Unlike a passive attacker, an ***active attacker*** relies on intercepting the communication between a given source and destination. Such interception is done aggressively by altering, modifying and deleting the given information and data being transmitted without the knowledge of the source and destination. Such an attack is very dangerous when used for example to inject a patient with a higher dosage of a drug, or when prescribing the wrong drugs, and thus, seriously risking patients' lives.

  - **Malicious & Rational Attackers:** ***Malicious attackers*** do not have a specific goal and do not look for specific results either. They launch their attacks simply because they can do it with the intention to disrupt an IoMT system. This can be done, for example, by transmitting false information to the data center in a specific geographical area. In contrast, ***rational attackers*** have a specific target which can have a very dangerous impact. In other terms, they are unpredictable and generally follow the passive class.
  - **Organized & Coordinated Attackers:** Cyber-attacks against IoMT can be organized or coordinated. ***Organized attacks*** are usually based on having prior knowledge of a given medical device or system before launching a cyber-attack against it. In fact, the aim is to either gain an unauthorized access or disclose sensitive information. ***Coordinated attacks*** are based on the cooperation and collaboration between insiders and outsiders. In fact, insiders are rogue/unsatisfied employees (Hospital IT, staff, nurses, receptionists, etc.) having an authorized access to the system and possibly install a malware. Malware types allow outsiders to have an elevated remote access or privilege and carry out a combined attack against a specific medical system. The attack might be carried out in order to hit the system's availability and prevent authorized medical personnel and patients from accessing medical records, book appointments, or disrupt medical operations.

- **Target:** A targeted attack is typically used for assassination or terrorism purposes. Such an attack targets a specific patient or a hospital for various reasons that could be political (assassinating a public figure), ideological, racial or religious reasons. The attackers' goal could be to target a minority group of patients or to target a foreign country with the aim of fueling racism, or spreading terrorism, or part of a cyber-warfare campaign linked to cyber-politics.
- **Scope:** the scope of an attack is related to the targeted area, which may be quantified as small scale or large scale. Typically, attackers try to extend their malicious actions to a large area [84,85] to increase the number of victims, such as patients in hospitals.
- **Impact:** the impact of an attack is quantified by the amount of damage it causes, along with its nature and its scope.
- **Capacity:** this refers to the protection required to prevent, mitigate, or reduce the damage associated with an attack.

4.2. Targeted IoMT's security aspects

IoMT security seems to be jeopardized by various types of cyber-attacks, which are divided and described depending on the security aspect that they target. As illustrated in Fig. 7, in this section we aim at reviewing the security attacks that target the IoMT data security, including its availability, confidentiality and integrity. On the other hand, we aim to dissect the security attacks that target the system security including user privacy, system availability, confidentiality/trust, authentication and integrity.

4.2.1. Data confidentiality attacks

In order to hit the confidentiality of IoMT data, gathering information is a must. Due to the open and public nature of IoMT wireless communications, patients are becoming more prone to being intercepted through confidentiality (sniffing) attacks. Therefore, the risk of personal and private information being either leaked, hijacked, modified or even stolen is seriously high. However, in order to achieve it, different passive attacks can be carried out. This includes eavesdropping, traffic analysis, and brute force attacks. Table 4 presents the main confidentiality attacks.

- **Eavesdropping Attacks** are typically based on gathering information and they are divided into two main types. The first one is **Passive Eavesdropping** [86], where wireless access points are scanned to identify which medical device is connected to them. The second type is the **Active Eavesdropping**, where the adversary can monitor incoming and outgoing data during transmission and Thus, gathering more information in a faster and easier manner.
- **Data Interception Attacks** occur when a man-in-the-middle attack is carried out. This allows the adversary to intercept data and re-transmit it at a later time [87]. This allows the attacker to eavesdrop the Address Resolution Protocol (ARP) request and keeps on repeating it in order to capture a handshake. This handshake is then used to obtain encryption keys and gain unauthorized access to medical systems and records.
- **Packet Capturing Attacks** or packet sniffing attacks include the capture of the transmitted medical data packets that are unencrypted and revealing their content including patients' medical conditions and passwords. Wireshark is a prime example of a network monitoring software tool.
- **Wiretapping Attacks** include hacking medical telecommunication and tele-healthcare devices to intercept real-time incoming/outgoing medical data.
- **Dumpster Diving Attacks** include searching through dumpsters and retrieving any medical information including papers and file thrown in the bin including patients records, medical prescriptions, staff names, etc. This is one of the main reasons why most file and data records are becoming paperless.

4.2.2. Social engineering (SE) attacks

Social engineering is a technique used to manipulate people through either baiting or pre-texting in order to lure people to give out information. This includes passwords, names, IDs, private information in order to proceed with a cyber-attack later on. Luring people can be easily achieved by relying on human emotions which seems to be easier than exploiting a system's vulnerability. Therefore, the attacker relies on people's curiosity, or lust, and sends infected adult pictures (phishing), for example, in order to gain access to medical systems or/and records. Different SE attacks are presented in Table 5.

- **Reverse Engineering Attacks:** A reverse social engineering attack is also known as a person-to-person attack [88]. This allows the attacker to masquerade himself as a technician trying to fix an issue in a hospital's medical system and gaining insight and physical access to the system. It also allows him to possibly upload a malware or detect vulnerabilities that can be exploited. In other cases, an attacker can masquerade himself as a person visiting a patient, asking questions in order to gain a better insight about the used medical systems and devices.
- **Error Debugging Attacks** are usually caused by an improper handling of error, which results into medical systems becoming vulnerable to various security problems [89,90]. Such exploitation can lead to internal error messages that target medical web servers, application servers, and web application environments by displaying database dumps, stack traces and error codes to the attacker. This would mainly result into a system call failure/crash, network timeout or unavailable database. This consumes a high amount of resources and causes a tremendous network overhead, preventing and disrupting the availability of medical services to patients.

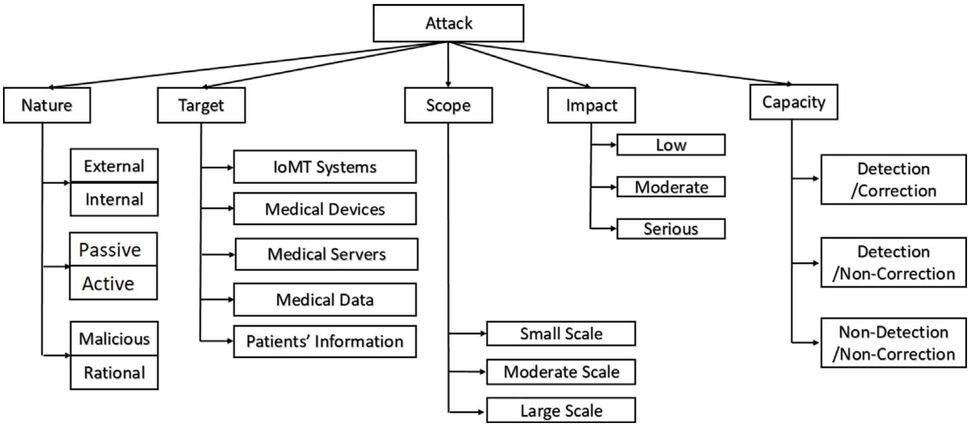

Fig. 6. Characteristics and profiles of attackers and its corresponding impact.

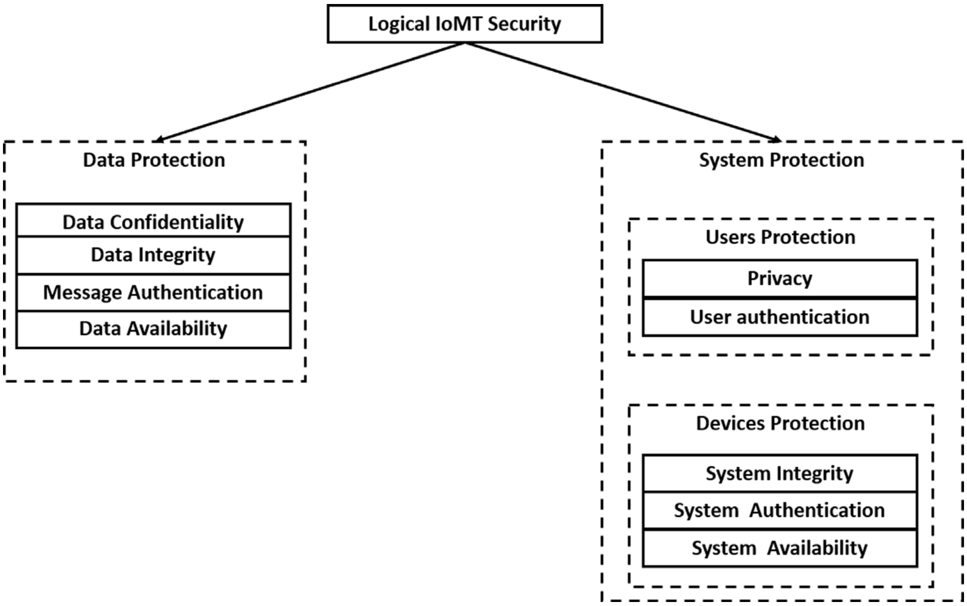

Fig. 7. IoMT security goals.

Table 4
Different types of data confidentiality attacks with their corresponding solutions.

Data confidentiality attack	Solutions	Possible reason(s)
Eavesdropping	Encryption	• Broadcast nature of messages via wireless channels • Unencrypted communication channel
Data interception	Encryption	• Non-Secure Channels • Open Wireless Communications
Packet capturing	Encryption	• Open Wireless Communications • Non-Secure Channels • Lack of Encryption
Wiretapping	• Secure Communications • Closed Communications	• Open Wireless Communication • Non-Secure Channels
Dumpster diving	• Enhanced Employee Training • Paperless Process	• Lack of Employee Training • Lack of Awareness

4.2.3. *Privacy attacks*

Ensuring patients' privacy is one of the most important challenges in IoMT. Preserving patients' privacy is mainly related to preventing the disclosure of their real identities, in addition to their location and information. This requires patients to keep their private information protected such as their identity, their behavior, their past and present location [91–93]. Moreover, in the following, the main privacy attacks are listed and described in Table 6.

- **Traffic Analysis Attacks:** TAA mainly affects patients' privacy in addition to their data confidentiality. This attack is extremely dangerous and consists of intercepting and analyzing the network traffic pattern(s), trying to infer useful

Table 5
Different types of social engineering attacks with their corresponding solutions.

Social engineering attack	Solutions	Possible reason(s)	Related threats
Social engineering	Training staff against baiting/pretexting	Poor training of employees	May affect the confidentiality and privacy.
Reverse social engineering	Training staff against strangers' questions	No identification and verification processes	Depends on the asked questions, primarily targets confidentiality and privacy. In addition, to affecting authentication and availability.
Error debug	Limit appearing information	Different error questions giving additional information	May affect (data/system's) confidentiality and privacy.

information. This is due to the fact that IoMT devices' activities can potentially reveal enough information, enabling an adversary to cause malicious harm to the medical devices.
More precisely, traffic analysis can target certain information that can be used to establish or facilitate new social engineering attacks.

- **Identity/Location Tracking Attacks:** The attacker spies on an IoMT device during its journey to discover the identity of the patient (relating the patient to a place of work or home). In fact, an attacker may get a trace of the IoMT devices' movements. Studying this trace can reveal the true identity of the patient, in addition to their personal information. Therefore, getting the identity of a given patient can put their privacy and possibly their life at risk.
  In order to preserve the privacy of any patient, the MAC and IP addresses must be constantly changed to avoid any possible identity disclosure and denial of service, or spoofing attack [84]. Hence the need to design some new algorithms to address the large memory-space dilemma. Therefore, each patient should be allocated a pool of certified pseudonyms obtained from a certificate authority [94,95]. The most popular attack is the Sybil attack. The pool of pseudonyms can be used to pretend they are for different patients whilst sending false messages to a data center. This includes false traffic jams, or false alerts forcing hospitals to react to a false event. The main authorities' goal is to ensure that the identities and their corresponding sensitive data are protected and verified during any communication attempt. In case of any issue, the system operators must interfere, however, it requires knowing the identity of the user (digital forensics). This indicates that a trade-off between privacy and digital forensics, indeed, exists.

4.2.4. Data integrity and message authentication attacks

Integrity attacks are based on the ability to alter the messages that are being transmitted in order to target the integrity of a system or data. Different attacks can be carried out to achieve this goal, such as injection attacks and data interception. Therefore, it is essential to secure and maintain the integrity of data as much as possible [96,97].

- **Message Tampering-Alteration Attacks:** The attacker here aims to break the data integrity of the exchanged messages. This happens when the attacker manipulates the received messages for his/her own goals [98]. This will result into doctors making wrong decisions that might compromise the health of patients.
  One of these security methods is using a message authentication algorithm such as cryptographic keyed hash function as HMAC to ensure data integrity and source authentication.
- **Malicious Data injection:** This kind of attack is generated from an entity that can be legal or can authenticate with the system. Thus, this can cause hazardous effects in the IoMT system and it may lead to fatal accidents [99], by creating a false message and transmitting it to the hospital data center or to doctors. The strategy of this attack is to prevent the real and correct messages from authorized users, and instead inject false messages into the network.
  To defend against such an attack, messages should be authenticated.
- **Malicious Script Injection Attacks:** Such attacks introduce false update script system where adversaries can mimic a legitimate server for system backup. This allows a given adversary to gain unauthorized access to any IoMT device and might introduce a backdoor [100].
- **Cloning And Spoofing Attacks** can be combined in order to carry out a more sophisticated attack [101] against a medical system or device. Cloning attacks duplicate the data spoofed, whilst spoofing attacks use the cloned data to gain unauthorized access [102].

Table 7 summarizes the main message integrity and authentication attacks.

4.2.5. Availability attacks

In order to target the availability of medical systems, different attacks are carried out to degrade the performance of medical systems and devices. As a result, the availability attacks can either target data availability or system availability.

- **Data Availability attacks:** The attacker aims to break the data availability of the exchanged messages by dropping these messages. This happens when the attacker manipulates the received messages for his/her own goals, which results into hospital data center or doctors missing important information about the patients' health conditions.
- **System Availability attacks:** The main system availability attacks are listed below and summarized inTable 8.
  - **Denial of Service Attacks (DoS):** In order to disrupt the availability of a given medical IoMT system or device, DoS attacks are initiated and launched, preventing legitimate patients from getting proper medications, and preventing nurses and doctors (GPs) from accessing medical information and records. This prevents real-time data from being sent and received through the disruption and interruption of service.
  - **Distributed Denial of Service Attacks (DDoS):** These attacks can also be simultaneously carried out from different geographical locations and from different countries. This can have a far greater impact on the availability of medical devices and systems resulting into a negative impact on the patients' lives with the inability to respond on time.
  - **De-Authentication Attacks:** Such attacks are usually carried out to ensure a single de-authentication attack against a given medical device. It can also be used in order to lead a mass de-authentication process, which prevents all connected devices from being operational either temporarily or permanently. This process also

Table 6
Different types of privacy attacks with their corresponding solutions.

Privacy attack	Solutions	Possible reason(s)
Traffic analysis	• VPNs & Proxies • Non-Linkability • Pseudonyms	• Source and destination information are not encrypted • Lack of secure channels • Weak encryption algorithm
Identity/Location tracking	• Anonymity • Non-Linkability • Pseudonyms	• Lack of secure channels • Location and identification parameters are not encrypted

Table 7
Different types of data integrity and message authentication attacks along their corresponding solutions..

Message integrity and authentication attack	Solutions	Possible reason(s)
• Message Tampering-Alteration • Malicious data injection • Malicious Script Injection • Cloning & Spoofing	• Keyed Hash Function (HMAC); • Message Authentication Algorithms	No data integrity and source authentication protection scheme

allows the capture of a handshake, which can be used later on to launch a cracking attack, which enables an adversary to gain unauthorized access to a medical system, device or even server.

- **Wireless Jamming** aims to severely interrupt and disrupt any established wireless communication of medical devices between patients and hospitals. More specifically, wireless networks are severely targeted [103] by a series of continuous denial of service attacks, which disrupts any communication attempt on secure and non-secure channels, depending on whether the jamming attack is selective or non-selective [104]. However, this attack can be mitigated through frequency hopping and frequency shifting, as described in [105].
- **Flooding Attacks:** they are based on overwhelming and exhausting the medical system's resources by injecting false information and data to flood the system with false data and information requests [106].
  - **ICMP Flooding Attacks** are an Internet Control Message Protocol (ICMP) flood or Ping flood attacks with a Denial-of-Service (DoS) ability that overwhelms a targeted medical device with ICMP echo-requests known as pings [107]. Attackers rely on exploited IoMT devices (zombies or bots) controlled by a bot master to conduct such type of attacks.
  - **SYN Flooding Attacks** or "half-open" attacks primarily target high-capacity IoMT devices since they rely on Transmission Control Protocol (TCP) services to communicate (i.e email/web servers) [108]. The aim of this attack is to cause a medical server to crash by exhausting the e-Healthcare server's memory reserve to make insecure connections available for further attacks.
  - **Black Nurse Attacks** are highly effective low bandwidth (15–18 Mbit/sec) ICMP attacks that target firewalls with high Central Processing Unit (CPU) load through denial of service attacks [109]. This attack results into preventing Local Area Network (LAN) users, including patients and medical staff from transmitting internet network traffic.
- **Delay Attacks:** They introduce high delays for high priority message transmissions. This offers the ability to either re-transmit them or not transmit them at all after the elapsed time.

4.2.6. Device/user authentication attacks

Authentication attacks aim to overcome passwords, which are classified as the first and primary line of defense, in order to gain access to a given system [110]. Usually, attacks are successful in many cases including when a given password is either too weak or too short, or is static. These attacks can either be encryption cracking (brute force, dictionary, birthday, or rainbow-table attacks), among other attack types mentioned in Table 9.

- **Man-in-the-Middle Attacks:** This attack is one of the main authentication attacks; it controls and monitors the communication between two legitimate parties, whilst altering the transmitted data. This attack can either be passive or active. It is considered as a passive attack when the attacker only intercepts and reads the exchanged messages between the two entities. On the other hand, it is considered as an active attack, if the attacker is able to alter, manipulate or/and modify the transmitted data or information without any of the devices' knowledge.
- **Brute Force Attacks** are based on an excessive search for all possible combinations that make up and crack a given password of a medical [111]. Such an attack aims to acquire patients' credentials and private medical information for fraud purposes. Most targeted devices include, but are not limited to, remote medical sensors and patient monitors [112].
- **Masquerading Attacks** occur when a wireless network relay node is exploited by a given attacker for malicious purposes. Such attack can constantly send false alarms about an emergency medical condition, and can disrupt the availability of medical services [113]. Moreover, masquerading attacks can modify a patient's medical condition and may result into injecting the wrong drug or an excessive medicine usage, which may result into the loss of human lives.
- **Replay Attacks** modify the control signal being transmitted to another medical device, especially once an attacker gains a high privilege to the system with the ability to control the system's signals. The adversary may either steal or/and intercept the transmitted information by redirecting it to another location. In some cases, physical damage can be achieved against a given system [106], including medical systems. System communications are recorded first before being 'replayed' later to the receiving device [101]. This can lead to either stealing, leaking or disclosing sensitive information to gain an unauthorized access and elevated privilege on a given medical system [114].
- **Cracking Attacks** are based on capturing a handshake through a de-authentication attack. Thus, luring the intended AP (Access Point) to respond back with a handshake.

Table 8
Different types of system availability attacks with their corresponding solutions.

Availability attack	Solutions	Possible reason(s)
Jamming	Frequency Hooping, direct sequence spread spectrum, beam-forming	Targets Access Points or wireless IoMT devices
Denial Of Service	Backup Devices	Lack of Backup Devices
Distributed Denial of Service (DDOS)	DDOS detection solutions. Increase the security levels of devices to avoid becoming bots.	Exploiting devices turning them into bots
De-authentication	Firewalls, Intrusion Detection Systems, Encryption	Captures a handshake to Launch DoS or Password Cracking Attack
Flood	Timestamps, Certificate Authority, IDS	Overwhelms & Exhausts IoMT's Resources through False Information Injection
Delay	Firewalls, Timestamps, IDS	Overwhelms & Prevent or Severely Delays any Transceiving of Medical Information

Once the handshake is captured, a password cracking attack is conducted against a given medical system or device. This allows the leakage of information and data disclosure.

- **Dictionary Attacks** usually take place when trying to gain access to a given medical system [115]. Attacks are usually successful when security measures are less tight than the security measures of a given IoT device. Such attacks occur by relying on a large set of dictionary words in an attempt to guess the password so that the adversary can gain access. In fact, such an attack type is exhaustive in terms of resources and time, and can take time from minutes to hours, and sometimes days. Brute force attacks are usually aimed at targeting a medical device where the security measures are weak [116]. In many cases, they still rely on a number combination including the personal identification number (PIN).
- **Rainbow Table Attacks** are usually aimed at targeting the password and its hash value relying on a technique process known as "fault and trial" through the use of reverse engineering. It usually contains a table of passwords along with their hashes, which is executed until a match is found. To overcome this problem, different solutions were presented in [117,118]. However, salt passwords can be a good solution to mitigate this type of attacks.
- **Session Hijacking Attacks** are also known as TCP Session Hijacking. This attack is achieved by using a Session sniffer that involves a packet sniffer capable of altering, capturing and reading the network traffic (header and data) between two parties. This includes users or/and devices alike. In fact, this attack can capture a valid Session ID (SID).
- **Birthday Attacks** are also due to users relying on weak hashing mechanisms, where two different passwords can have the same hash. Such weakness can easily be exploited to gain an unauthorized access to any medical system. A suggested hash function balance was presented in [119]. However, Secure Hash Algorithm (E.g SHA-3 and SHA-512) mechanisms remain the best solution against such attacks.

4.2.7. Malware attacks

IoMT devices can be targeted by various forms of malware [120,121], such as Trojans, worms, viruses, spyware, backdoor, botnet, and many others. This is due to many reasons such as their wireless and permanent connection to the Internet, in addition to a weak security protection and monitoring. A malware is based on the exploitation of a software weakness, vulnerability, or/and security gap. This leads to the possibility of having a backdoor to a given medical device or system. Moreover, it can lead to an unauthorized access to IoMT devices, leakage, disclosure, modification or deletion of sensitive patient information. In the event of a malware succeeding in creating back-doors into IoMT devices, attackers can use them to initiate other types of attacks or to deny access to their services (e.g. Denial of Sleep attacks).

Clearly, one of the main security requirements for IoMT devices is to prevent malware attacks. This aspect is evident by the recent cyber attacks, which exploited IoT devices to form botnets (e.g. Mirai). Another type of a malware attack that can affect IoMT devices is ransomware [122,123], which causes the denial of their services. In this context, advanced malware types, based on encryption or polymorphic techniques, impose serious threats [124]. As such, to prevent malware attacks, an anti-malware software is required, and we present in Section 5.2.6 the different intrusion detection techniques that can be implemented in order to detect, track down and prevent any possible malware attack. In the following, we list the main types of malware attacks that can target IoMT systems and devices:

- **Spyware Attacks:** The main purpose of a spyware is to collect and gather information about patients and to send them to either a third party or to sell them through the deep dark web. This is done by keeping users under constantly covert surveillance. Actually, spyware may collect enough information about a given patient for possible assassination. They can be also used as key-loggers to steal patients' credentials [125].
- **Ransomware Attack** Insufficient attention is paid to IoT ransomware, which can lead to catastrophic results [126] compared to traditional ransomware [122]. The classic ransomware model is simply not feasible in the IoT case because, in most cases, IoT data is stored in the fog and/or cloud and not at the device level. IoT ransomware consists of locking IoT devices and asking for ransom from their owners to unlock them [127]. Normally, in traditional ransomware, attackers employ the user interface (screen display) to warn the user to pay the ransom. However, there is no display interface for a significant percentage of IoT devices. In this case, attackers attempt to discover their owners emails or hacking the app that controls the compromised IoT devices. IoT ransomware is efficient since it is timely, critical, and reversible. Therefore, attackers choose scenario where users do not have enough time and are not in place to reset the device or counter the ransomware effects. In these cases, users are more than willing to pay the ransom. Unfortunately, IoMT devices are attractive targets for ransomware [128]. Thus, locking the functions of some devices such as pacemakers, drug infusion pumps, etc., can lead to catastrophic results since patients would be seriously harmed or even dead if these devices are not unlocked in due time.
- **Worm Attacks** Worms are likely the most destructive and dangerous type of malware in the IoMT case [129].

Table 9
Different types of system authentication attacks with their corresponding solutions.

Authentication attack	Solutions	Possible reason(s)	Related threats
Man-in-the-Middle	Multi-Factor authentication scheme	Poor authentication scheme (one factor)	Depending on attacker goals, it might affect the data's integrity, confidentiality and availability.
Masquerading	Multi-Factor authentication scheme	Poor authentication scheme (one factor)	May affect data's confidentiality.
Cracking	Multi-Factor authentication scheme	Poor authentication scheme (one factor)	may affect the data's confidentiality and integrity.
Replay	• Timestamp or a new random number for each session connection • Multi-Factor authentication scheme	Weakness in the authentication protocol	May affect system's availability.
Dictionary	• Strong password • sufficient size of secret key	Weak password and one authentication factor	May affect the data's confidentiality & integrity
Brute force	• Strong and long password • sufficient size of secret key • Multi-Factor authentication scheme	• Weak password • and one authentication factor	May affect data's confidentiality and integrity
Rainbow Table	Long Salt Passwords	• Weak Usernames/Password • Short Salt Passwords	May affect data's confidentiality and integrity
Birthday	Secure Hash Algorithm	Weak Hashing	May affect data's confidentiality and integrity
Session Hijacking	• Encryption • Sniffing Filters	• Lack of/Poor Encryption • Non-Secure Channels	May affect data's confidentiality, integrity and availability

Worms are a form of malware that self-replicates vertically over a connected device, after exploiting the device's existing vulnerabilities. Thus, they are capable of self-propagating without human intervention. They can impact all data and devices' security services (confidentiality, integrity, and availability), which may result in critical loss of data or life risks. For example, they can be designed to target a given industrial control system [130]. A recent malicious Internet worm, "dubbed", which targeted IoT devices was presented in [131]. Unfortunately, worms can be implemented and used against IoMT devices in order to gather information, damage or even destroy a given device. Thus, in the IoMT case, if insecure devices are installed, they can compromise the security of the whole medical system once they are infected by worms, which can propagate automatically in the whole system by exploiting existing vulnerabilities. Note that worms also can be combined with other malware types such as ransomware and botnets to propagate through the whole IoMT network [132].

- **Botnet Attacks** These attacks are based on exploiting vulnerabilities within IoMT devices [133,134], and turning them into bots, awaiting orders from the adversary through command-and-control to send fake or false information concerning patients. They can also be used to bring the whole medical system down through DoS or DDoS attacks [6,135]. In fact, in many cases, such attacks are aimed at disclosing sensitive information and using them for malicious or personal gains. An example of such attacks is the Mirai attack [136], which infected IoT devices by malware to form botnets and to conduct DDoS attacks on the network servers, infrastructure, etc. On Sept 19, 2016, the first Mirai incident targeted OVH, one of the largest European hosting providers. Since then, an increased rate of attacks were launched by skilled and unskilled attackers given that the source code of this attack was made available online. Thus, in the medical domain, implants, smart pens, monitors, temperature sensors, infusion and insulin pumps, etc. are wireless devices that can be compromised by Mirai, if the convenient security measures are not in place. Consequently, these devices can be used as bots to attack the medical systems. Note that the Mirai attack has new mutated versions and there is a continuous effort in creating new and more powerful versions of this attack.
- **Remote Access Trojan Attacks (RAT):** RAT attacks occur through the exploitation of a medical system's vulnerability, weakness or security gap in a targeted medical system. Such attacks are based on evading all security procedures and countermeasures by gaining a covert unauthorized access as a backdoor. This leads to overcoming all of the security measures employed. It is mainly achieved by bypassing the authentication process. The most infamous attack was the operation Shady RAT [137].
- **Logic Bomb Attacks:** Logic bombs are classified as small programs that logically explode after reaching a certain date or time [138], damaging the medical systems' components such as IoMT devices.

All malware attacks and their solutions are summarized in Table 10.

4.2.8. Implementation attacks

Different implementation attacks on medical systems are presented in this section, including the side channel attacks, fault attacks, and timing attacks.

- **Side Channel Attacks** can possibly occur due to IoMT embedded systems having very limited physical properties. Moreover, they are used to recover the secret key using power consumption, differential power consumption or electromagnetic analysis. In fact, IoMT devices with Physical non-cloneable Functions (PUF) can guard against different implementation attacks.
- **Fault Attacks** target a physical electronic device by stressing the device by external means. This includes the increase/decrease of voltage to generate errors, which mostly leads to a security failure [139].
- **Timing Attacks** are classified as side channel attacks where an attacker attempts to compromise a cryptosystem by analyzing the needed execution time of cryptographic algorithms. In addition, a timing attack is a security exploitation, where an attacker discovers security vulnerabilities surrounding the computer or network system. Moreover, timing attacks are also used to target medical devices that use OpenSSL [140].

  This attack can become inefficient when using the "time stamping mechanism" for packets of delay-sensitive applications. However, this proposition encountered the problem of time synchronization between entities [141,142].

Table 10
Different types of malware attacks with their corresponding solutions.

Malware attack	Solutions	Possible reason(s)	Related threats
Botnet	Botnet detection solution (anti-malware), pen-testing, intrusion detection	A logical collection of exploited internet-connected devices or IoMT devices	Depends on the attacker's target (confidentiality, integrity, authentication and/or availability)
Worm & Viruses	Anti-virus, anti-malware, pen-testing, intrusion detection	Relies on computer network security failures	Depends on the attacker's (confidentiality, integrity, authentication and/or availability)
Spyware	Use antivirus and anti-spyware solutions, update OS, ensure higher security and privacy levels, intrusion detection	Part of other software or downloads on file-sharing sites	Primarily targets privacy and data confidentiality but it can used for other purposes such as availability, authentication and/or integrity.
Remote Access Trojan	Keep antivirus software up to date, block unused ports, intrusion detection	Downloaded invisibly with a program or update software	Depends on the attacker's (confidentiality, integrity, authentication and/or availability)
Rootkit	Appropriate system configuration, strong authentication, patch and configuration management, intrusion detection	Exploits and targets either the kernel, or the user application space gains root privileges.	Primarily targets system's authentication
Ransomware	Up-to-date Anti-Virus/Anti-Malware, Avoid Using Personal Information, Enhanced System's Security, Higher Awareness	Weak Passwords, Weak Multi-Factor, Paying Ransoms	Targets system's Authentication and Availability, in addition to data confidentiality and privacy

All implementation attacks along with their solutions are summarized in Table 11.

To defend the listed attacks, several security measures should be taken, including technical and non-technical ones. In the next section, we review the existing security solutions for IoMT data and systems. In addition, we include the security practices and guidelines that should be followed to ensure IoMT systems and data confidentiality, integrity, privacy, etc.

5. IoMT security measures

Overcoming the rising IoMT security issues and challenges is a challenging task. However, mitigating them can be achieved by implementing multiple security measures, some being technical and others non-technical measures.

5.1. Non-technical security measures

This section is dedicated to highlight the different non-technical security measures that can be applied according to the needs. This includes training the staff and safeguarding the patients' private medical health records.

Training the medical and IT staff could be accomplished in three different ways: raising awareness, conducting technical training, and raising the education level as illustrated in Fig. 8.

- **Raising Awareness:** It is highly necessary and recommended to raise awareness among medical employees and staff, mainly the IT department in order to know and identify an occurring attack from normal network behavior. However, this is not enough, as there is a higher need for defining what is a threat, risk and a vulnerability. This offers them the chance to identify a risk from a threat. It also offers the possibility to assess the likelihood and impact of a risk. Once a risk is assessed, it is also essential to explain how to mitigate it and use the right security measures to deal with any threat and reduce its risk.
- **Technical Training:** Raising awareness is not enough, it is equally important to start training the medical staff and employees of the IT department, right after the teaching phase. The training must be divided into seven different phases, starting with:
  - **Identification Phase** where the IT is capable of identifying a suspicious behavior from an abnormal behavior.
  - **Confirmation Phase** that is based on the ability to confirm that an attack is occurring.
  - **Classification Phase** that is based on the ability to identify the type of the occurring attack.
  - **Reaction or Responsive Phase** is based on the ability of the Computer Emergency Response Team (CERT) to quickly react to a given attack using the right security defensive measures and prevent an attack from escalating.
  - **Containment Phase** is based on containing the attack incident and overcoming it.
  - **Investigation Phase** is the implementation of forensic evidences where an investigation process takes place to identify the cause of the attack [143], its impact and damage.
  - **Enhancement Phase** is based on learning from the lessons of previous attacks.
- **Raising Education Level:** The current focus must be targeted towards raising the level of education, especially for those in the IT domain. This is based on teaching and educating cyber-security and IT staff the necessary techniques to classify each attack and what it targets (confidentiality, integrity, availability, and/or authentication). Attackers are also divided into insiders or outsiders. However, it is important to assess the level of damage of an attack caused by an insider, along with the possibility of a remote or outsider attack. Afterwards, it is also highly recommended to educate them on how to evaluate the possibility of a risk from occurring (likelihood/impact). It is also important to know what encryption or cryptographic technique can or should be used to prevent any alteration or interception. To limit the possibility of insider attacks, the right authorization and authentication techniques should be applied, along with the best Intrusion Detection Systems (IDS) in order to detect any attack based on either signature, anomaly or behavior.

5.2. Technical security measures

In this section, we discuss the technical security measures that should be put in place to ensure an end-to-end secure IoMT system. Thus, the following subsections discuss techniques that aim at ensuring IoMT data and systems security.

Table 11
Different types of implementation attacks with their corresponding solutions.

Implementation attack	Solutions	Possible reason(s)	Related threats
Side channel attack	Hardware countermeasure (PUF) and software randomization processes	Limitations of physical properties related to the embedded devices	**It may lead to secret key recovering and consequently affect the data confidentiality.**
Fault attack	uses protected hardware and Spatial Retreat	Memory & disk manipulation	**May affect the System integrity. This type of attacks modifies the execution code to recover the secret key and consequently affect both data authentication and confidentiality.**
Timing attack	Constant Cryptographic Computations Execution Time, Independent Cryptographic Algorithm	Possible cryptographic software or algorithm Exploitation	**May cause the secret key recovering and consequently affect data's confidentiality.**

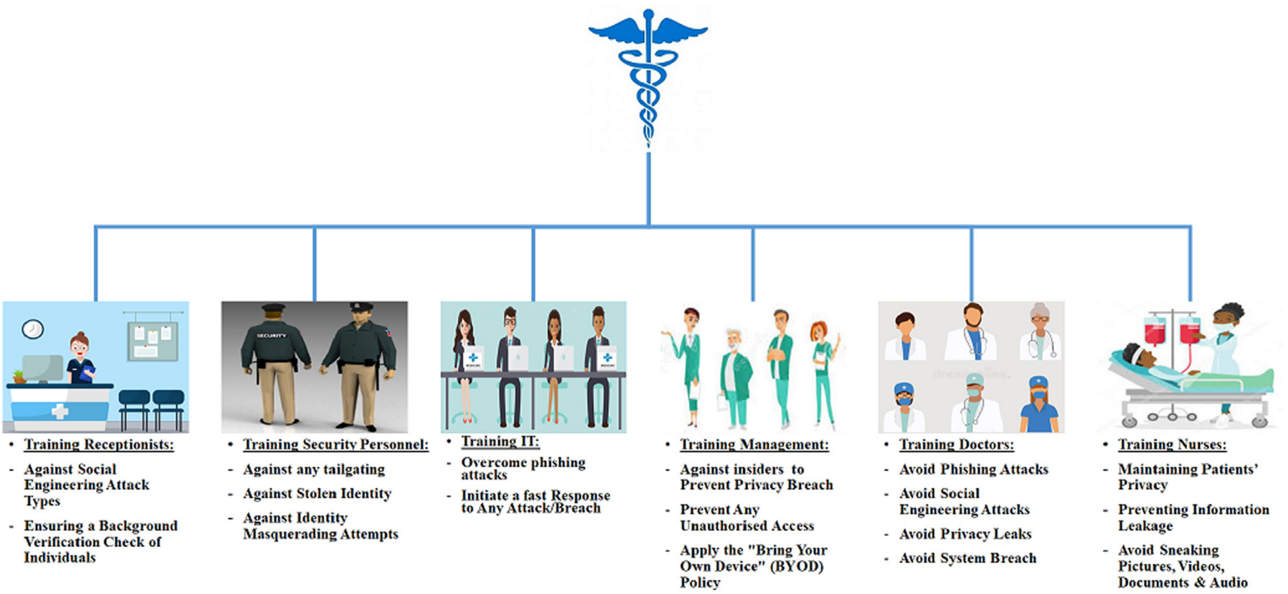
• Training Receptionists:
- Against Social Engineering Attack Types
- Ensuring a Background Verification Check of Individuals
• Training Security Personnel:
- Against any tailgating
- Against Stolen Identity
- Against Identity Masquerading Attempts
• Training IT:
- Overcome phishing attacks
- Initiate a fast Response to Any Attack/Breach
• Training Management:
- Against insiders to Prevent Privacy Breach
- Prevent Any Unauthorised Access
- Apply the "Bring Your Own Device" (BYOD) Policy
• Training Doctors:
- Avoid Phishing Attacks
- Avoid Social Engineering Attacks
- Avoid Privacy Leaks
- Avoid System Breach
• Training Nurses:
- Maintaining Patients' Privacy
- Preventing Information Leakage
- Avoid Sneaking Pictures, Videos, Documents & Audio

Fig. 8. IoMT staff training.

5.2.1. *Multi-factor identification and verification*

In order to prevent any possible unauthorized access to IoMT systems, it is important to ensure a strong identification and verification mechanism. The best solution is to rely on biometric systems. There is also the need for a database to store the biometric templates safely and securely for future use [144]. However, achieving identification and verification requires several biometric techniques, which can be divided into physical and behavioral biometric techniques [144].

- **Physical Biometric Techniques:** Secure physical biometric techniques can be adopted and used to safeguard and maintain patients' medical privacy without being prone to any insider threat. This includes facial recognition, retina scan, or iris scan.
  - **Facial Recognition:** Facial recognition managed to prove a high verification rate [145]. Hence, it was used in order to recognize a person's facial structure, using a specialized digital video camera that identifies and measures the face's structure. This also includes the distance between the triangle of eyes, nose and mouth. Hence, it is able to verify legitimate users from non-legitimate users by comparing a scanned face with the authorized faces registered in the database.
  - **Retina Scan:** A retinal recognition scan is based on analyzing the blood vessel region located behind the human eye. It proved to be a very accurate and secure verification method by [146].
  - **Iris Scan** proved to be essential for both identification and verification purposes, due to its ability to generate accurate and precise measurements [147]. Iris scan operates by analyzing and scanning the colored tissue around a specific eye pupil to check if it matches the stored data to either grant access or not.
- **Behavioral Biometric Technique:** A secure behavioral biometric technique that can be used for both identification and verification phases is the hand geometry. Such biometric systems rely on hand measurements, including palm size, hand shape, and finger dimensions [144]. Then, it is compared to the set of stored data in a database to verify users. If there is match, a given staff will be granted access. If not, access will be denied. However, such systems are only limited to one-to-one systems [148]. In fact, current systems are capable of differentiating between a living hand and a dead hand. This prevents adversaries from trying to deceive the system and gain any illegal access [149].

5.2.2. *Multi-factor authentication techniques*

Venka & Gupta [150] presented a survey that focused on patients' privacy violation, with the reliance on encryption, authentication and access control mechanisms as countermeasures. Authentication is classified as the first line of defense that authenticates the source and destination alike. In fact, authentication can be a single-factor authentication that only relies on a password as the only security measure, which is not preferable. It can also be a two-factor authentication that relies on another security measure aside from the password in order to access a given system. Finally, it can be a multi-factor authentication where a third security mechanism is required in order to access a system. Therefore, authentication plays a key role in providing security for the accessible resources on a given network.

Authentication can be either centralized where two nodes authenticate themselves through a trusted third party, or it can be distributed where two nodes use a pre-defined secret key to authenticate each other, without relying on a trusted third party.

Furthermore, in [151], Halperin et al. presented a cryptography-based key-exchange authentication mechanism that relies on external radio frequency rather than batteries as an energy source. This approach can be used in order to constantly prevent any unauthorized personnel from gaining access [152]. The out-of-band authentication was also deployed in a number of wearable devices including mainly heart rate and blood pressure monitors [153]. It is based on the use of additional channels including audio and visual channels to generate a key to encrypt and secure the body sensor communications in a given network [154]. In [155], Ankarali et al. presented a physical layer authentication technique which relies on pre-equalization. Furthermore, an enhanced dual-factor user authentication scheme was presented and used by both authors in [156,157] in order to protect WSNs. According to [158], Das et al. presented a smart-card-based password authentication scheme for WSNs [159], which mainly lacked user's anonymity [160]. In [161], Li et al. presented their own advanced temporal credential-based security scheme which included a mutual authentication and key agreement for Wireless Sensor Networks (WSNs). Gope et al. presented another authentication scheme based on a realistic lightweight anonymous authentication protocol used for securing real-time application data access for WSN [162]. Kumar et al. [163] attempted to develop a privacy-preserving two-factor authentication framework exclusively for WSNs to overcome various attack types.

5.2.3. Authorization techniques

An assigned authorization must be based on offering the least privilege. Hence, the Role-Based Access Control (RBAC) model is adopted. This model offers the least privilege for a given medical staff or employee to perform a given task with the least (necessary) permissions and functionalities to accomplish a specific task.

- **T-Role-Based Access** (T-RBAC) is mainly designed for cloud computing environments, especially where medical data is stored [164]. T-RBAC is a proper access control model for Smart Health-care Systems [165]. In addition, T-RBAC also stands for Temporal Role Based Access Control, and can be spatio-temporal [166], intelligent [167], and generalized [168]. It is also capable of validating any needed access permission for any medical user according to the assigned role and tasks. In fact, T-RBAC can be divided between two task types, the workflow tasks that need to be completed in a particular order (this requires an active access control), and the non-workflow tasks, which can be completed in any order that requires a passive access control.

5.2.4. Availability techniques

The importance of maintaining availability against any possible disruption or/and interruption of signals is a must. However, maintaining the server's availability requires the implementation of computational devices that act as backup devices, along a verified backup and Emergency Response Plans (ERP) in case of any sudden system failure.

- **Against Jamming:** Jamming can take many forms (see Fig. 9), including DoS, DDoS, or/and de-authentication. In the event of jamming attacks, several medical services would be severely affected, especially with the disruption and interruption of medical services. This can lead to the disruption and prevention of communications between medical devices and the doctor or GP, which leads to missing updates of patients' health records and hence, health complications. Furthermore, with these medical services being brought down by a jamming attack, first responders will not be able to arrive to the scene on time. This would increase the potential of a given patient being prone to strokes that can possibly lead to their death. For this specific purpose, different security measures must be implemented in order to overcome any attack that would target the availability of any given system. For example, having backup computational medical devices and servers is crucial. In fact, medical devices must be available 24/7 in order to ensure the necessarily medical requirements and needed attention. Furthermore, backup devices must be quick to respond in real-time and activated in case of any emergency that threatens the availability of a given medical system. In fact, additional security measures can be taken into consideration, including Channel surfing, spatial retreat, and priority messages [169], which can be very useful against wireless denial of service attacks. This can be a good countermeasure for medical devices, especially in the IoMT domain.

5.2.5. Honeypots

Honeypot systems are really useful when it comes to detecting attackers, their targets (see Fig. 10), tools and used methods. However, the reliance on static honeypot systems is challenging. Hence, the need for a dynamic honeypot system configuration. Although there are no specific honeypots for IoMT, some honeypots are being employed in IoT systems and these might also be useful in the IoMT system as well. In [170], Luo et al. mentioned that building honeypots for IoT devices is challenging using traditional methods. Therefore, they presented an automatic and intelligent way to collect potential responses using a scanner and a leverage machine technique to learn the correct behavior during an interaction with an attacker. Their evaluation revealed that their proposed system can improve the session interaction with the attackers to capture further attacks.

In [171], La et al. developed a game theoretic model to analyze deceptive attacks and defense problems in a honeypot enabled IoT network. In fact, a Bayesian belief update scheme was used in their repeated game. Their presented game model and simulation results showed that whenever facing a high concentration of active attackers, the defender's best interest was to heavily deploy honeypots. This allowed the defenders to use a mixed defensive strategy that keeps the attacker's successful attack rate low. Finally, their game theoretic approach may be suitable for medical health-monitoring systems, and sensor networks.

In [172], Dowling et al. presented an analysis of the results from bespoke ZigBee simulated honeypot deployed on Secure Shell (SSH). This simulated honeypot is used to detect and analyze automated and random attack types before being examined and identified. Brute-force and botnet attacks provided a better material for examination, unlike individual and dictionary attacks. Therefore, these attacks managed to treat the honeypot as an SSH device and concentrated on compromising it. This was done by showing interest in the honey-tokens to manipulate them. Individual attacks have shown an interest in a small number of files that were already downloaded and sandboxed. This also included the scripts that were analyzed, rather than having any specific knowledge towards Zigbee networks. In [173],

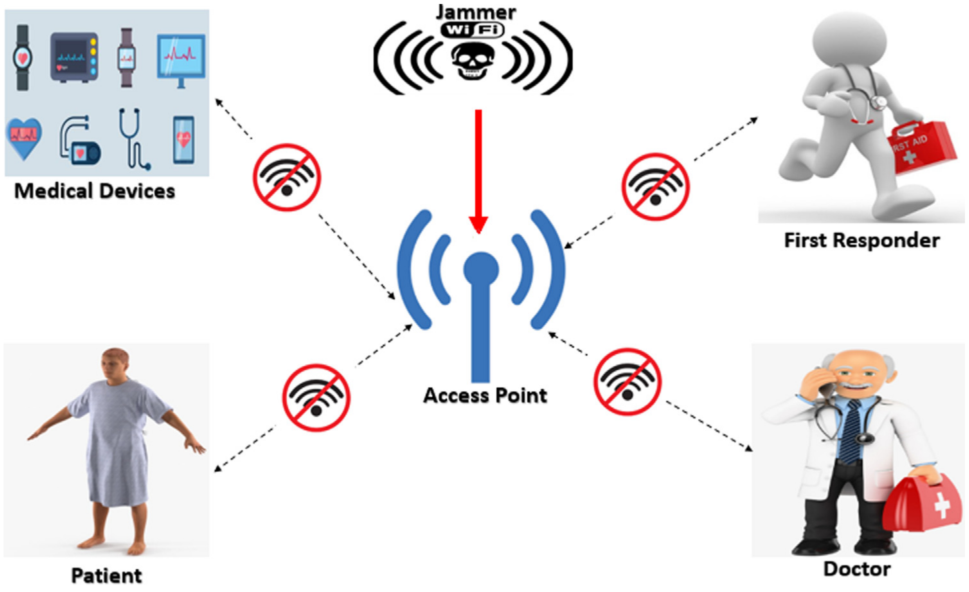

Fig. 9. An example of possible jamming attacks & their impact on iomt systems including: Data center, first responders, doctors & patients — Targeting main iomt communication channels.

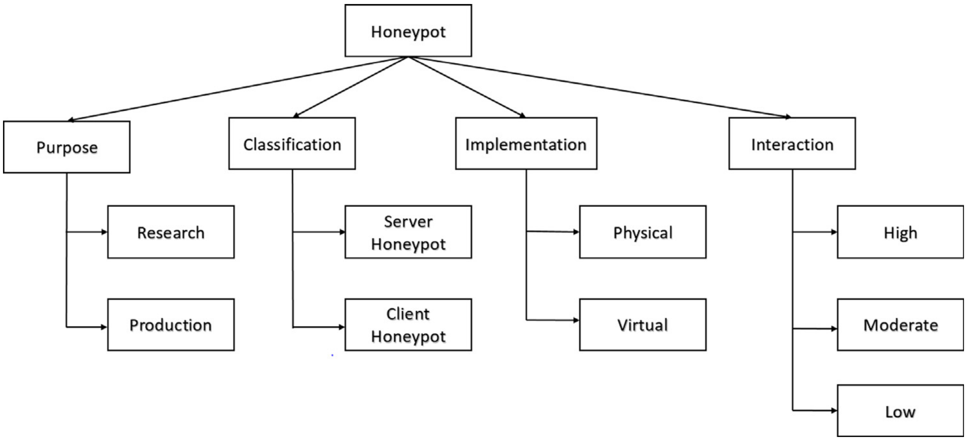

Fig. 10. Honeypot taxonomy based on 4 metrics: Purpose, classification, implementation, & interaction.

Anirudh et al. managed to conduct a detailed study on how a DoS attack is conducted against IoT systems. This included how they can be averted by a honeypot relying on a verification system to maintain the efficiency of transmitted and received data. Their outcome demonstrated the capability of their presented scheme to secure an IoT system through the implementation of honeypots. Their future work includes deploying honeypots to overcome DDoS and botnet attacks.

5.2.6. Lightweight intrusion detection systems

IoMT devices are prone to different types of security threats and challenges. To protect IoMT systems against intruders, the activities of IoMT devices must be monitored and analyzed. Typically, an IDS is the first line of defense towards detecting attacks. The different IDS types that can be applied within IoMT systems are Host-based IDS (HIDS), and Network-based IDS (NIDS). While HIDS is attached to a given IoMT device to monitor any possible malicious activity, NIDS monitors the network traffic of several IoMT devices towards detecting any malicious activity.

IoMT systems and networks should be protected by implementing IDS to detect abnormal activities as early as possible and to initiate the right actions to stop any incident. An IDS can be either anomaly-based, signature-based, or specification-based, as shown in Fig. 11. Signature-based and specification-based detection methods require low overhead compared to the anomaly-based one. Unfortunately, due to the limited computing power and the high number of interconnected devices, a traditional anomaly-based IDS is not efficient in the IoMT case.

Anomaly-based detection is the most efficient in detecting zero-day attacks, which is not possible via signature-based or specification-based detection methods. Developing a lightweight anomaly-based IDS is essential for the detection of unknown attacks within the IoMT context. Such lightweight techniques will be used to make prompt decisions in a resource-constrained environment, as is the case in IoMT networks. Without an efficient anomaly IDS, IoMT devices can be compromised leading to drastic effects especially for patients. This raised a real security concern about current IoMT deployments in general, and the need for a robust and lightweight IDS. Research and industrial communities are still facing challenges in designing a reliable and efficient IDS for IoT systems since large amounts of data are supposed to be handled in a real-time manner. Lightweight and hybrid cooperative IDS with hybrid placement and hybrid detection techniques are candidate solutions that can make IoT networks resilient against various types of attacks including zero-day attacks.

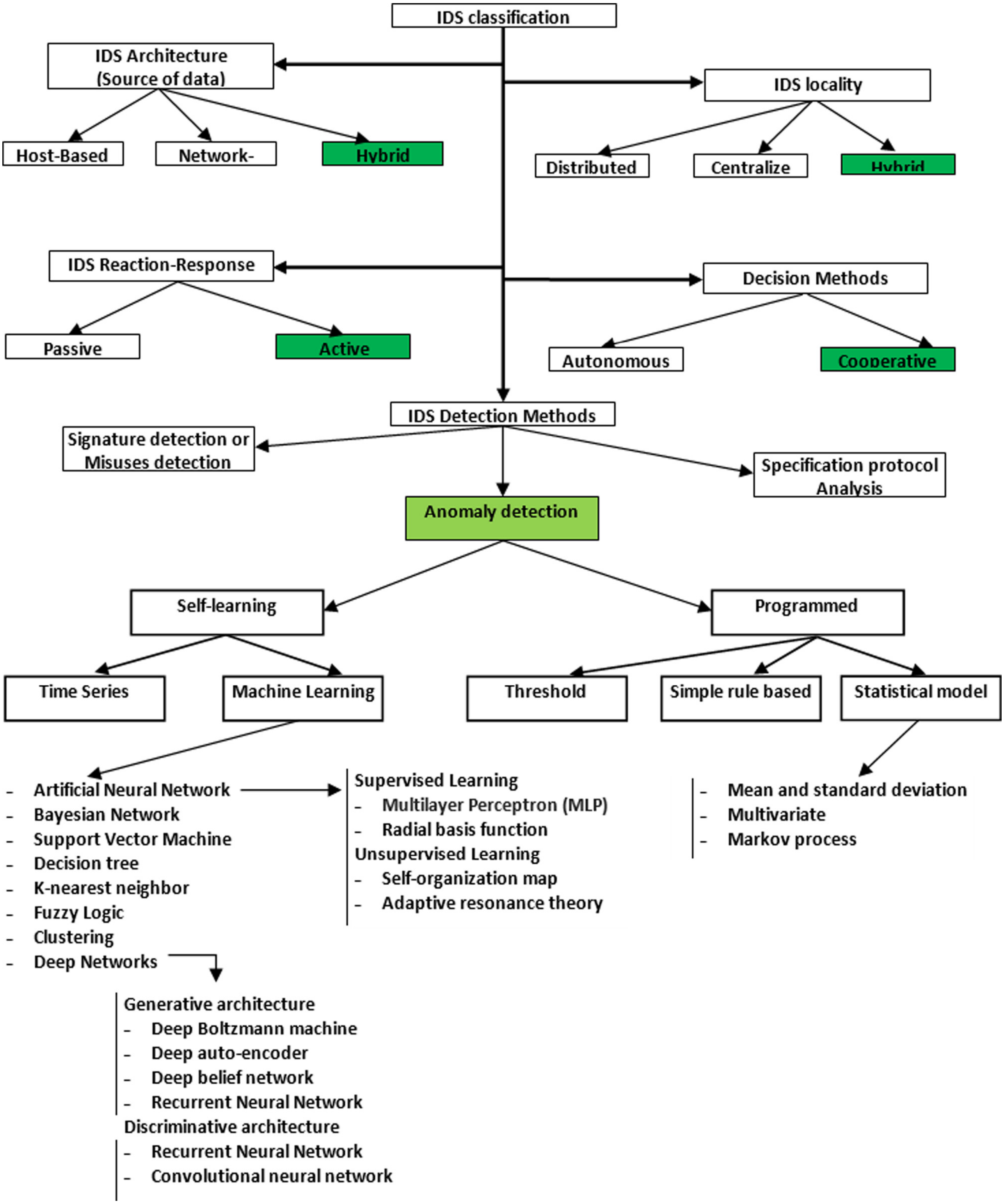

Fig. 11. Modern IDS classification based on 5 factors: Architecture, Locality, reaction–response, decision class & detection methods.

6. Suggestions & recommendations

Failing to implement encryption would lead to intercepting, modifying, and even deleting data beyond recovery. As such, encryption techniques, and more so dynamic encryption, must be implemented to safeguard the data and ensure its privacy and confidentiality (see Fig. 12). Moreover, since most attacks have occurred due to social engineering or phishing attacks, a budget must be allocated to raise the awareness and to conduct training of medical staff, and to raise their technical knowledge to identify any potential phishing or social/reverse engineering attack. Moreover, the IT staff should undergo more specialized training in order to secure, maintain and safeguard the privacy of stored sensitive confidential medical data and information. Additionally, a strong multi-factor authentication must be employed (see Fig. 13).

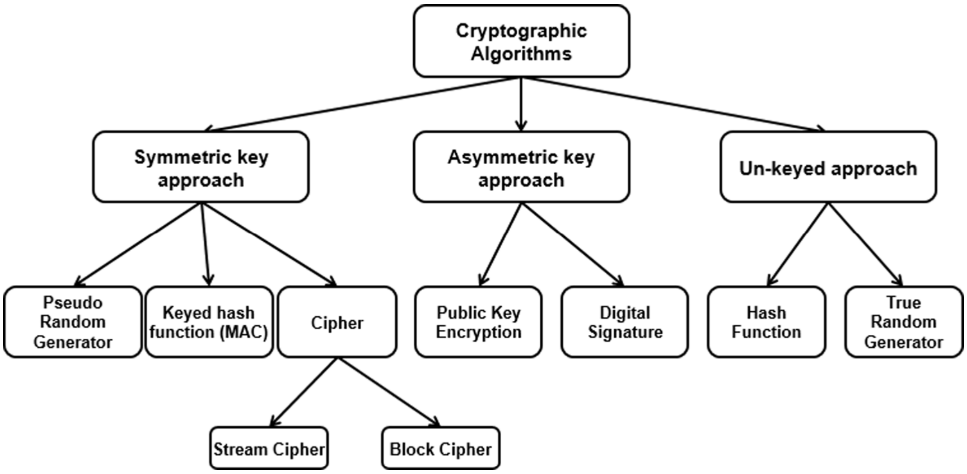

Fig. 12. Existing cryptographic algorithms.

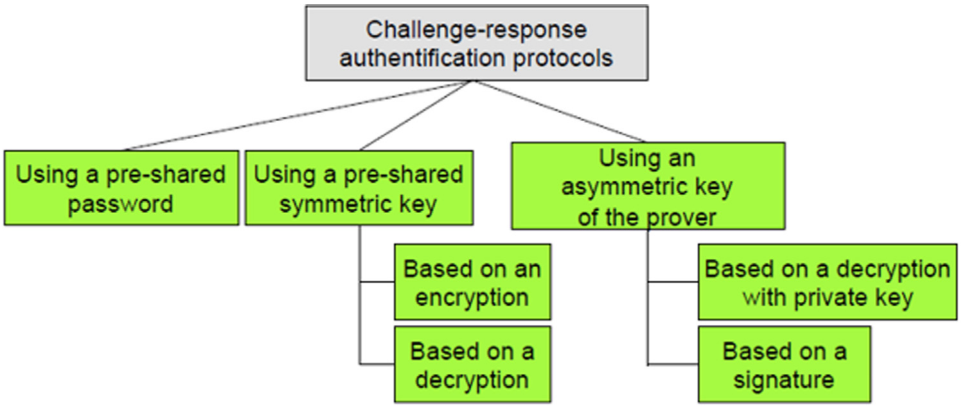
Challenge-response authentification protocols
Using a pre-shared password
Using a pre-shared symmetric key
Using an asymmetric key of the prover
Based on an encryption
Based on a decryption
Based on a decryption with private key
Based on a signature

Fig. 13. Existing authentication cryptographic protocol techniques.

Note that there is a high level of mistrust among patients who are raising serious concerns about their privacy, especially that the recent attacks disclosed private medical information and data about patients. Therefore, it is crucial to establish trust and it should be given a high priority. Aside from protecting and securing data by ensuring both security and privacy, it is also important to maintain a high level of accuracy of medical robotics operations, to avoid errors that may lead to unnecessary loss of life. In addition, lightweight security mechanisms are required for authentication and encryption to ensure a safe transmission of real-time medical data, especially for resource-constrained smart healthcare devices. This requires ensuring the right trade-off between IoMT's system performance, and security and privacy mechanisms.

In the following, we list the main recommendations towards securing IoMT systems and data.

6.1. Lightweight cryptographic algorithms

In general, security is based on cryptographic algorithms (see Fig. 12) to ensure data confidentiality, integrity and availability, with source authentication, and non-repudiation. However, implementing security and privacy countermeasures introduces an overhead, which is considered high for some type of IoMT devices. Many related works were presented towards reducing the required latency and resources for these countermeasures. In some scenarios, medical data must be exchanged in real-time, without any delay, such is the case of live monitoring and exchanging surveillance data. Moreover, the existing algorithms would quickly drain the battery life of small medical sensors, or small endpoints within IoMT. To address this issue, the cryptographic algorithms proposed in [9,29,34,55,83,93,115,117,124,138,141,167,174–178] rely on a dynamic structure instead of the typical static structure, whereby the cipher primitives change for each new input message, and thus, they require a small number of rounds to achieve the required security level, which would require multiple rounds in a static structure. In [179–181], the technique meets the expected requirements and ensures a high level of security that is both essential and mandatory for IoMT.

6.2. Lightweight authentication protocols

A survey on the existing authentication protocols for IoMT is presented in [11,12,182], and typically, such protocols use cryptographic algorithms as a basic element. This includes a hash function (with or without key), as well as symmetric and asymmetric cryptographic algorithms (see Fig. 13). Designing an efficient cryptographic algorithm for IoMT would lead to reducing the required latency and resources of the corresponding computation. Also, it is important to reduce the required number of exchanged messages, and the size of the messages in the authentication step.

6.3. Layered security architecture

The security layers in IoMT, as shown in Table 12, should consist of three main layers:

Table 12
Recommended security layers & components.

Accuracy layer	
Trust sub-layer	• Accurate Medical Applications • Least Error Prone • Patients Trust • Trusted Medical Device/Equipment • Certified Authority • Trusted Third Party
Prevention layer	
Authentication sub-layer	• User/Device Authentication: • Multi-factor Authentication • Physical Protection • Strong and Variable Password • Source Authentication and Message Integrity • Access Control
Privacy sub-layer	• Patients Privacy • Anonymity (Pseudonymity) • Proxies VPN • Preserving Privacy at Cloud (Differential Privacy, Secret Sharing, Homomorphic Encryption)
Data confidentiality sub-layer	• Encryption Algorithm
Defensive layer	
Detection sub-layer	• Intrusion Detection Systems (Anti-malware) • SIEM • Honeypots • Data System Integrity
Correction sub-layer	• Intrusion Prevention Systems • Firewalls • Data Backup • Alternative Devices and Configuration

(1) **Accuracy Layer:** Accuracy of medical operations and tasks heavily relies on ensuring a three-way mutual trust that is set between medical staff (nurses and doctors) and medical applications and operations, medical staff and patients, patients and applications and operations.

- **Trust Sub-Layer:** it requires the adoption of the most accurate medical applications, which must be highly accurate in a real-time manner, with zero tolerance to errors. Moreover, digital medical devices and equipment must also be verified through a certified authority, which may or may not be linked to a trusted third party.

(2) **Prevention Layer** is required to prevent any attack from within the organization, and to reduce the likelihood of any remote attack to disclose the patients' medical data. This requires establishing the right authentication, privacy and confidentiality mechanisms.

- **Authentication Sub-Layer** requires establishing a multi-factor authentication that relies on a strongly dynamic and variable password, and on a biometric technique that is unique for each patient, which makes any attempt to breach into patients' data extremely difficult. This can also be applied to medical staff to establish the right access control mechanism by establishing the least privilege per employee's role. Moreover, user/device authentication must be established to ensure a physical protection when using medical applications to prevent any physical tampering. Finally, source authentication and message integrity must be established by relying on a certified authority between the hospital and the patient.
- **Privacy Sub-Layer** requires taking into consideration patients' privacy as a high priority. This requires allowing patients to adopt anonymity and pseudonymity, by ensuring that they use a well-established private connection (Proxies and VPN) when being linked to medical websites or applications. Moreover, medical IT staff must rely on privacy preserving data mining techniques based on cloud and fog computing, aside the adoption of traditional privacy preserving data mining techniques such as differential privacy (Signal-to-Noise), secret sharing [183], and homomorphic encryption.
- **Data Confidentiality Sub-Layer** must be maintained at all times to guard against passive attacks. This requires the adoption of lightweight cryptographic algorithms, as well as relying on quantum cryptography to protect high-value assets.

(3) **Defensive Layer:** to maintain a secure e-health environment, early detection measurements are required before any corrective measures are established.

- **Detection Sub-Layer** requires establishing and employing the most advanced up-to-date anti-malware and anti-viruses, along AI-based solutions linked to dynamic and hybrid Intrusion Detection Systems Security Information and Event Management (SIEM), and dynamic honeypots. This will ensure an early and highly accurate detection rate.
- **Correction Sub-Layer** must be maintained as the second line-of-defense to mitigate and overcome security attacks. This includes an enhanced dynamic Intrusion Prevention Systems, dynamic and next generation firewalls, while ensuring a secure and verified data backup, with alternative devices being available for necessary computational requirements.

7. Conclusions

Despite its advantages, IoMT is prone to a variety of attacks, issues and challenges that mainly target the privacy of patients and the confidentiality, integrity and availability of medical services.

In this paper, we presented and discussed the main problems, challenges and drawbacks facing IoMT, along with the different security measures that can be implemented to safeguard and secure the IoMT domains and their associated assets, which include medical devices, systems, and medical CPSs. Moreover, different frameworks, taxonomies and approaches were presented to ensure a more enhanced and robust IoMT, and improve the patients' health and experience. Furthermore, it is important to secure the different wireless communication protocols that the IoMT relies on. Finally, it is essential to maintain a high level of security, privacy, trust and accuracy. Hence, it is highly essential and recommended to train medical and IT staff so that they do not fall victims to physical or/and cyber-attacks. As a summary, the aim of is paper is to tighten the ties between different technical solutions and non-technical solutions to ensure a much more sophisticated, secure and efficient system in all IoMT domains.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was made possible by NPRP Grant no. 10-1205-160012 from the Qatar National Research Fund, a member of the Qatar Foundation. The statements made herein are solely the responsibility of the authors.

References

[1] Ekaterina Balandina, Sergey Balandin, Yevgeni Koucheryavy, Dmitry Mouromtsev, IoT use cases in healthcare and tourism, in: Business Informatics, CBI, 2015 IEEE 17th Conference on, volume 2, IEEE, 2015, pp. 37–44.

[2] Christoph Thuemmler, Chunxue Bai, Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare, Springer, 2017.

[3] Zhibo Pang, Geng Yang, Ridha Khedri, Yuan-Ting Zhang, Introduction to the special section: convergence of automation technology, biomedical engineering, and health informatics toward the healthcare 4.0, IEEE Rev. Biomed. Eng. 11 (2018) 249–259.

[4] Ryan A. Beasley, Medical robots: current systems and research directions, J. Robot. 2012 (2012).

[5] Jacob Rosen, Blake Hannaford, Doc at a distance, IEEE Spectr. 43 (10) (2006) 34–39.

[6] Lei Zhang, Shui Yu, Di Wu, Paul Watters, A survey on latest botnet attack and defense, in: Trust, Security and Privacy in Computing and Communications , TrustCom, 2011 IEEE 10th International Conference on, IEEE, 2011, pp. 53–60.

[7] Yanping Zhang, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang, Hongmei Deng, A survey of cyber crimes, Secur. Commun. Netw. 5 (4) (2012) 422–437.

[8] J. Sathish Kumar, Dhiren R. Patel, A survey on internet of things: Security and privacy issues, Int. J. Compt. Appl. 90 (11) (2014).

[9] Robert Mitchell, Ing-Ray Chen, A survey of intrusion detection techniques for cyber-physical systems, ACM Comput. Surv. 46 (4) (2014) 55.

[10] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, A survey of intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017) 25–37.

[11] Dylan Sey, A survey on authentication methods for the Internet of Things, PeerJ Prepr. 6 (2018) e26474v1.

[12] Michal Trnka, Tomas Cerny, Nathaniel Stickney, Survey of authentication and authorization for the Internet of Things, Secur. Commun. Netw. 2018 (2018).

[13] Sumanta Kuila, Namrata Dhanda, Subhankar Joardar, Sarmistha Neogy, Jayanta Kuila, A generic survey on medical big data analysis using internet of things, in: First International Conference on Artificial Intelligence and Cognitive Computing, Springer, 2019, pp. 265–276.

[14] Anna Challoner, Gheorghe H. Popescu, Intelligent sensing technology, smart healthcare services, and internet of medical things-based diagnosis, Am. J. Med. Res. 6 (1) (2019) 13–18.

[15] Seungjin Kang, Hyunyoung Baek, Eunja Jung, Hee Hwang, Sooyoung Yoo, Survey on the demand for adoption of Internet of Things (IoT)-based services in hospitals: Investigation of nurses' perception in a tertiary university hospital, Appl. Nurs. Res. 47 (2019) 18–23.

[16] Tathagata Adhikary, Amrita Deb Jana, Arindam Chakrabarty, Saikat Kumar Jana, The Internet of Things (IoT) augmentation in healthcare: An application analytics, in: International Conference on Intelligent Computing and Communication Technologies, Springer, 2019, pp. 576–583.

[17] Ovunc Kocabas, Tolga Soyata, Mehmet K. Aktas, Emerging security mechanisms for medical cyber physical systems, IEEE/ACM Trans. Comput. Biol. Bioinform. 13 (3) (2016) 401–416.

[18] Carmen C.Y. Poon, Yuan-Ting Zhang, Shu-Di Bao, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, IEEE Commun. Mag. 44 (4) (2006) 73–81.

[19] Krishna K. Venkatasubramanian, Ayan Banerjee, Sandeep Kumar S. Gupta, PSKA: Usable and secure key agreement scheme for body area networks, IEEE Trans. Inf. Technol. Biomed. 14 (1) (2010) 60–68.

[20] Alliance ZigBee, Zigbee-2006 specification, 2006, http://www.zigbee.org/.

[21] Pravin Bhagwat, Bluetooth: technology for short-range wireless apps, IEEE Internet Comput. 5 (3) (2001) 96–103.

[22] Wi-Fi Alliance, Wi-fi certified wi-fi direct, White paper, 2010.

[23] Klaus Doppler, Mika Rinne, Carl Wijting, Cássio B. Ribeiro, Klaus Hugl, Device-to-device communication as an underlay to LTE-advanced networks, IEEE Commun. Mag. 47 (12) (2009).

[24] Vikram Chandrasekhar, Jeffrey G. Andrews, Alan Gatherer, Femtocell networks: a survey, IEEE Commun. Mag. 46 (9) (2008).

[25] Feng Ye, Yi Qian, Rose Q. Hu, Energy efficient self-sustaining wireless neighborhood area network design for smart grid, IEEE Trans. Smart Grid 6 (1) (2015) 220–229.

[26] Xiaojun Wang, Leroy White, Xu Chen, Yiwen Gao, He Li, Yan Luo, An empirical study of wearable technology acceptance in healthcare, Ind. Manage. Data Syst. (2015).

[27] Hatice Ceylan Koydemir, Aydogan Ozcan, Wearable and implantable sensors for biomedical applications, Annu. Rev. Anal. Chem. 11 (2018) 127–146.

[28] Shivayogi Hiremath, Geng Yang, Kunal Mankodiya, Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare, in: 2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies, MOBIHEALTH, IEEE, 2014, pp. 304–307.

[29] Alan Naditz, Telemedicine named one of space race's top tech breakthroughs, Telemedicine e-Health 15 (8) (2009) 735–736.

[30] Shelten Gee Jao Yuen, James Park, Atiyeh Ghoreyshi, Anjian Wu, User identification via motion and heartbeat waveform data, Google Patents, US Patent 9,851,808, 2017.

[31] Mary Beth Pinto, Arpan Yagnik, Fit for life: A content analysis of fitness tracker brands use of Facebook in social media marketing, J. Brand Manag. 24 (1) (2017) 49–67.

[32] Roland Asmar, Validation of the automatic blood pressure measurements device, the omron evolv (hem-7600 te)® in pregnancy according to the modified european society of hypertension international protocol (esh-ip), 2017.

[33] Stanislav V. Kasl, Sidney Cobb, Health behavior, illness behavior and sick role behavior: I. health and illness behavior, Arch. Environ. Health 12 (2) (1966) 246–266.

[34] J.A. Nijboer, J.C. Dorlas, J. Lubbers, The difference in blood pressure between upper arm and finger during physical exercise, Clin. Physiol. 8 (5) (1988) 501–510.

[35] Anthony G.A. Aggidis, Jeffrey D. Newman, George A. Aggidis, Investigating pipeline and state of the art blood glucose biosensors to formulate next steps, Biosens. Bioelectron. 74 (2015) 243–262.

[36] Melanie Swan, Sensor mania! the Internet of Things, wearable computing, objective metrics, and the quantified self 2.0, J. Sens. Actuator Netw. 1 (3) (2012) 217–253.

[37] Joseph Tran, Rosanna Tran, John R. White, Smartphone-based glucose monitors and applications in the management of diabetes: an overview of 10 salient ''apps'' and a novel smartphone-connected blood glucose monitor, Clin. Diabetes 30 (4) (2012) 173–178.

[38] Elliot Krames, Implantable devices for pain control: spinal cord stimulation and intrathecal therapies, Best Pract. Res. Clin. Endocrinol. Metab. 16 (4) (2002) 619–649.

[39] Robert Wang, Gordon Blackburn, Milind Desai, Dermot Phelan, Lauren Gillinov, Penny Houghtaling, Marc Gillinov, Accuracy of wrist-worn heart rate monitors, Jam. Cardiol. 2 (1) (2017) 104–106.

[40] Olli Komulainen, Heart rate monitor, Google Patents, US Patent App. 29/131,645, 2001.

[41] Paul Marrow, Manolis Koubarakis, Rolf-Hendrik van Lengen, F. Valverde-Albacete, Erwin Bonsma, Jesús Cid-Suerio, Anıbal R. Figueiras-Vidal, Ascensión Gallardo-Antolín, Cefn Hoile, Theodoros Koutris, et al., Agents In Decentralised Information Ecosystems: the Diet Approach, 2001.

[42] Kevin Hung, Yuan-Ting Zhang, B. Tai, Wearable medical devices for telehome healthcare, in: The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, volume 2, IEEE, 2004, pp. 5384–5387.

[43] National Research Council, et al., The Role of Human Factors in Home Health Care: Workshop Summary, National Academies Press, 2010.

[44] Lora Perry, Robert Malkin, EFfectiveness of Medical Equipment Donations to Improve Health Systems: How Much Medical Equipment Is Broken in the Developing World? Springer, 2011.

[45] Biomedical equipment list - MedShare, 2019, https://www.medshare.org/biomedical-equipment/.

[46] 10 pieces of medical equipment all hospitals need, 2017, https://www.futurehealthconcepts.com/blog/posts/10-pieces-of-medical-equipment-all-hospitals-need.html.

[47] Sana Ullah, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem, Ziaur Rahman, Kyung Sup Kwak, A comprehensive survey of wireless body area networks, J. Med. Syst. 36 (3) (2012) 1065–1094.

[48] Daan J. Van De Velde, Niels O. Schiller, Claartje C. Levelt, Vincent J. Van Heuven, Mieke Beers, Jeroen J. Briaire, Johan H.M. Frijns, Prosody perception and production by children with cochlear implants, J. Child Lang. 46 (1) (2019) 111–141.

[49] Henri Lorach, Ryad Benosman, Olivier Marre, Sio-Hoi Ieng, José A. Sahel, Serge Picaud, Artificial retina: the multichannel processing of the mammalian retina achieved with a neuromorphic asynchronous light acquisition device, J. Neural Eng. 9 (6) (2012) 066004.

[50] Rohit Suvarna, Sushant Kawatkar, Dhanamma Jagli, Internet of medical things [IoMT], Int. J. 4 (6) (2016).

[51] Leila A. Haidari, Shawn T. Brown, Marie Ferguson, Emily Bancroft, Marie Spiker, Allen Wilcox, Ramya Ambikapathi, Vidya Sampath, Diana L. Connor, Bruce Y. Lee, The economic and operational value of using drones to transport vaccines, Vaccine 34 (34) (2016) 4062–4067.

[52] Aaron Pulver, Ran Wei, Clay Mann, Locating AED enabled medical drones to enhance cardiac arrest response times, Prehospital Emerg. Care 20 (3) (2016) 378–389.

[53] Ming Li, Russell H. Taylor, Spatial motion constraints in medical robot using virtual fixtures generated by anatomy, in: Robotics and Automation, 2004. Proceedings. ICRA'04. 2004 IEEE International Conference on, volume 2, IEEE, 2004, pp. 1270–1275.

[54] Colin J. McCarthy, Raul N. Uppot, Advances in virtual and augmented reality—exploring the role in health-care education, J. Radiol. Nurs. (2019).

[55] Brendan William Munzer, Mohammad Mairaj Khan, Barbara Shipman, Prashant Mahajan, Augmented reality in emergency medicine: A scoping review, J. Med. Internet Res. 21 (4) (2019) e12368.

[56] Steve Balian, Shaun K. McGovern, Benjamin S. Abella, Audrey L.. Blewer, Marion Leary, Feasibility of an augmented reality cardiopulmonary resuscitation training system for health care providers, Heliyon 5 (8) (2019) e02205.

[57] Fei Jiang, Yong Jiang, Hui Zhi, Yi Dong, Hao Li, Sufeng Ma, Yilong Wang, Qiang Dong, Haipeng Shen, Yongjun Wang, Artificial intelligence in healthcare: past, present and future, Stroke Vasc. Neurol. 2 (4) (2017) 230–243.

[58] Jackie Hunter, Adopting AI is essential for a sustainable pharma industry, Drug Discov. World (2016) 69–71.

[59] Pratik Shah, Francis Kendall, Sean Khozin, Ryan Goosen, Jianying Hu, Jason Laramie, Michael Ringel, Nicholas Schork, Artificial intelligence and machine learning in clinical development: a translational perspective, NPJ Digit. Med. 2 (1) (2019) 69.

[60] P. Agrawal, Artificial intelligence in drug discovery and development, J. Pharmacovigil. 6 (2018) 1–2.

[61] Bao Tran, Personal emergency response (per) system, Google Patents, US Patent 8,531,291, 2013.

[62] Steffen Clarence Pauws, Mohammad Hossein Nassabi, Linda Schertzer, Tine Smits, Jorn OP DEN BUIJS, Patrick William Van Deursen, Personal emergency response system with predictive emergency dispatch risk assessment, Google Patents, US Patent App. 15/317,440, 2017.

[63] Steven R. Peabody, System containing location-based personal emergency response device, Google Patents, US Patent 8,116,724, 2012.

[64] Asimina Kiourti, Konstantinos A. Psathas, Konstantina S. Nikita, Implantable and ingestible medical devices with wireless telemetry functionalities: A review of current status and challenges, Bioelectromagnetics 35 (1) (2014) 1–15.

[65] Daniel R. Marshall, Swallowable data recorder capsule medical device, Google Patents, US Patent 6,632,175, 2003.

[66] William Robert Bandy, Brian Glenn Jamieson, Kevin James Powell, Kenneth Edward Salsman, Robert Charles Schober, John Weitzner, Michael R. Arneson, Ingestible endoscopic optical scanning device, Google Patents, US Patent 8,529,441, 2013.

[67] Xinyue Liu, Christoph Steiger, Shaoting Lin, German Alberto Parada, Ji Liu, Hon Fai Chan, Hyunwoo Yuk, Nhi V. Phan, Joy Collins, Siddartha Tamang, et al., Ingestible hydrogel device, Nature Commun. 10 (2019).

[68] Shannon L. Toohey, Alisa Wray, Warren Wiechmann, Michelle Lin, Megan Boysen-Osborn, Ten tips for engaging the millennial learner and moving an emergency medicine residency curriculum into the 21st century, West. J. Emerg. Med. 17 (3) (2016) 337.

[69] Fendy Santoso, Stephen J. Redmond, Indoor location-aware medical systems for smart homecare and telehealth monitoring: state-of-the-art, Physiol. Meas. 36 (10) (2015) R53.

[70] Sophie McFarland, Anne Coufopolous, Deborah Lycett, The effect of telehealth versus usual care for home-care patients with long-term conditions: A systematic review, meta-analysis and qualitative synthesis, J. Telemedicine Telecare (2019) 1357633X19862956.

[71] Peter Cullin, Thomas Bergdahl, A telecare system, Google Patents, US Patent App. 16/310,127, 2019.

[72] Nazish Saeed, Mirfa Manzoor, Pouria Khosravi, An exploration of usability issues in telecare monitoring systems and possible solutions: a systematic literature review, Disabil. Rehabil. (2019) 1–11.

[73] Kevin Anderson, Oksana Burford, Lynne Emmerton, Mobile health apps to facilitate self-care: a qualitative study of user experiences, PLoS One 11 (5) (2016) e0156164.

[74] Minhee Kang, Eunkyoung Park, Baek Hwan Cho, Kyu-Sung Lee, Recent patient health monitoring platforms incorporating Internet of Things-enabled smart devices, Int. Neurourol. J. 22 (Suppl 2) (2018) S76.

[75] George W. Clark, Michael V. Doran, Todd R. Andel, Cybersecurity issues in robotics, in: Cognitive and Computational Aspects of Situation Management ,CogSIMA, 2017 IEEE Conference on, IEEE, 2017, pp. 1–5.

[76] Andrea Peterson, Yes, Terrorists Could Have Hacked Dick Cheney's Heart, Washington Post, 2013.

[77] Kevin Kelly, Better than human: Why robots will—and must—take our jobs, Wired, 2012, http://www.wired.com/2012/12/ff-robots-will-take-our-jobs/. (Accessed 4 August 2014).

[78] John D. Birkmeyer, Therese A. Stukel, Andrea E. Siewers, Philip P. Goodney, David E. Wennberg, F. Lee Lucas, Surgeon volume and operative mortality in the United States, New Engl. J. Med. 349 (22) (2003) 2117–2127.

[79] Luis Ayala, Active medical device cyber-attacks, in: Cybersecurity for Hospitals and Healthcare Facilities, Springer, 2016, pp. 19–37.

[80] Joyce Sensmeier, Harnessing the power of artificial intelligence, Nurs. Manag. 48 (11) (2017) 14–19.

[81] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, Silvana Andreescu, Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: Opportunities and challenges, in: 2015 IEEE International Conference on Services Computing, SCC, IEEE, 2015, pp. 285–292.

[82] Allan Turner, Kenneth Glantz, Julie Gall, A practitioner-researcher partnership to develop and deliver operational value of threat, risk and vulnerability assessment training to meet the requirements of emergency responders, J. Homel. Secur. Emerg. Manag. 10 (1) (2013) 319–332.

[83] Rim Moalla, Houda Labiod, Brigitte Lonc, Noemie Simoni, Risk analysis study of its communication architecture, in: Network of the Future, NOF, 2012 Third International Conference on the, IEEE, 2012, pp. 1–5.

[84] D. Senie, P. Ferguson, Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing, Network (1998).

[85] Pete Bagnall, R. Briscoe, Alan Poppitt, Taxonomy of Communication Requirements for Large-Scale Multicast Applications, Technical report, 1999.

[86] David D. Coleman, David A. Westcott, Cwna: Certified Wireless Network Administrator Official Study Guide: Exam Pw0-105, John Wiley & Sons, 2012.

[87] Daojing He, Sammy Chan, Mohsen Guizani, Drone-assisted public safety networks: The security aspect, IEEE Commun. Mag. 55 (8) (2017) 218–223.

[88] Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda, Calton Pu, Reverse social engineering attacks in online social networks, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2011, pp. 55–74.

[89] Patrick Schaumont, Fault Attacks on Embedded Software: Threats, Design, and Mitigation.

[90] Bilgiday Yuce, Fault Attacks on Embedded Software: New Directions in Modeling, Design, and Mitigation (Ph.D. thesis), Virginia Tech, 2018.

[91] Lucila Ohno-Machado, Paulo Sérgio Panse Silveira, Staal Vinterbo, Protecting patient privacy by quantifiable control of disclosures in disseminated databases, Int. J. Med. Inform. 73 (7–8) (2004) 599–606.

[92] Nicolas P. Terry, Protecting patient privacy in the age of big data, UMKC L. Rev. 81 (2012) 385.

[93] Cherilyn G. Murer, Protecting patient privacy, Public Law 104 (2002) 191.

[94] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmuller, Luca Delgrossi, Trust issues for vehicular ad hoc netw., in: Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, IEEE, 2008, pp. 2800–2804.

[95] Junggab Son, Donghyun Kim, Rasheed Hussain, Alade Tokuta, Sung-Sik Kwon, Jung-Taek Seo, Privacy aware incentive mechanism to collect mobile data while preventing duplication, in: Military Communications Conference, MILCOM 2015-2015 IEEE, IEEE, 2015, pp. 1242–1247.

[96] Nolan Jones, J.D. Sherry, System and method for authenticating a user using a graphical password, Google Patents, US Patent 8,347,103, 2013.

[97] Yogendra C. Shah, Andreas Schmidt, Vinod K. Choyi, Lakshmi Subramanian, Andreas Leicher, Multi-factor authentication to achieve required authentication assurance level, Google Patents, US Patent App. 14/786,688, 2016.

[98] Chun-Wei Yang, Tzonelih Hwang, Tzu-Han Lin, Modification attack on QSDC with authentication and the improvement, Internat. J. Theoret. Phys. 52 (7) (2013) 2230–2234.

[99] Yao Liu, Peng Ning, Michael K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. 14 (1) (2011) 13.

[100] Md Ashfaqur Rahman, Hamed Mohsenian-Rad, False data injection attacks with incomplete information against smart power grids, in: Global Communications Conference, GLOBECOM, 2012 IEEE, Citeseer, 2012, pp. 3153–3158.

[101] Sarah Spiekermann, Ethical IT Innovation: A Value-Based System Design Approach, Auerbach Publications, 2015.

[102] Huiyong Wang, Minglu Zhang, Jingyang Wang, Design and implementation of an emergency search and rescue system based on mobile robot and WSN, in: Informatics in Control, Automation and Robotics, CAR, 2010 2nd International Asia Conference on, volume 1, IEEE, 2010, pp. 206–209.

[103] Satish Vadlamani, Burak Eksioglu, Hugh Medal, Apurba Nandi, Jamming attacks on wireless networks: A taxonomic survey, Int. J. Prod. Econ. 172 (2016) 76–94.

[104] Alejandro Proano, Loukas Lazos, Selective jamming attacks in wireless networks, in: 2010 IEEE International Conference on Communications, IEEE, 2010, pp. 1–6.

[105] Kanika Grover, Alvin Lim, Qing Yang, Jamming and anti-jamming techniques in wireless networks: a survey, Int. J. Ad Hoc Ubiquitous Comput. 17 (4) (2014) 197–215.

[106] Zubair A. Baig, Abdul-Raoof Amoudi, An analysis of smart grid attacks and countermeasures, J. Commun. 8 (8) (2013) 473–479.

[107] Harshita Harshita, Detection and prevention of ICMP flood DDOS attack, Int. J. New Technol. Res. 3 (3) (2017).

[108] Mitko Bogdanoski, Tomislav Suminoski, Aleksandar Risteski, Analysis of the SYN flood DoS attack, Int. J. Comput. Netw. Inf. Secur. 5 (8) (2013) 1–11.

[109] Yuquan Shan, George Kesidis, Daniel Fleck, Angelos Stavrou, Preliminary study of fission defenses against low-volume DoS attacks on proxied multiserver systems, in: 2017 12th International Conference on Malicious and Unwanted Software, MALWARE, IEEE, 2017, pp. 67–74.

[110] John Clark, Jeremy Jacob, Attacking authentication protocols, High Integr. Syst. 1 (1996) 465–474.

[111] Chee-Wooi Ten, Govindarasu Manimaran, Chen-Ching Liu, Cybersecurity for critical infrastructures: Attack and defense modeling, IEEE Trans. Syst. Man Cybern. A 40 (4) (2010) 853–865.

[112] Emma McMahon, Ryan Williams, Malaka El, Sagar Samtani, Mark Patton, Hsinchun Chen, Assessing medical device vulnerabilities on the Internet of Things, in: 2017 IEEE International Conference on Intelligence and Security Informatics, ISI, IEEE, 2017, pp. 176–178.

[113] Pardeep Kumar, Hoon-Jae Lee, Security issues in healthcare applications using wireless medical sensor networks: A survey, sensors 12 (1) (2012) 55–91.

[114] Lukas Grunwald, New Attacks Against RFID-systems, GmbH Germany, 2006.

[115] Junghyun Nam, Juryon Paik, H.-K. Kang, Ung Mo Kim, Dongho Won, An off-line dictionary attack on a simple three-party key exchange protocol, IEEE Commun. Lett. 13 (3) (2009) 205–207.

[116] Jung-Sik Cho, Sang-Soo Yeo, Sung Kwon Kim, Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, Comput. Commun. 34 (3) (2011) 391–397.

[117] Arvind Narayanan, Vitaly Shmatikov, Fast dictionary attacks on passwords using time-space tradeoff, in: Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM, 2005, pp. 364–372.

[118] Ruhma Tahir, Huosheng Hu, Dongbing Gu, Klaus McDonald-Maier, Gareth Howells, Resilience against brute force and rainbow table attacks using strong icmetrics session key pairs, in: Communications, Signal Processing, and their Applications, ICCSPA, 2013 1st International Conference on, IEEE, 2013, pp. 1–6.

[119] Mihir Bellare, Tadayoshi Kohno, Hash function balance and its impact on birthday attacks, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2004, pp. 401–418.

[120] Andrei Costin, Jonas Zaddach, IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies, BlackHat USA, 2018.

[121] Jason R.C. Nurse, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese, Smart insiders: exploring the threat from insiders using the internet-of-things, in: 2015 International Workshop on Secure Internet of Things, SIoT, IEEE, 2015, pp. 5–14.

[122] Ben Dickson, The IoT ransomware threat is more serious than you think – IoT Security Foundation, https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/.

[123] Amin Azmoodeh, Ali Dehghantanha, Mauro Conti, Kim-Kwang Raymond Choo, Detecting crypto-ransomware in IoT networks based on energy consumption footprint, J. Ambient Intell. Humaniz. Comput. 9 (4) (2018) 1141–1152, http://dx.doi.org/10.1007/s12652-017-0558-5.

[124] Kurt Nimmo, Will stuxnet malware be used in false flag attack, 2010, Infowars.com.

[125] Younghwa Lee, Kenneth A. Kozar, Investigating factors affecting the adoption of anti-spyware systems, Commun. ACM 48 (8) (2005) 72–77.

[126] David Balaban, Ransomware and the Internet of Things | cyber defense magazine, 2019, https://www.cyberdefensemagazine.com/ransomware-and-the-internet-of-things/. (Accessed on 11/13/2019).

[127] S.R. Zahra, M. Ahsan Chishti, Ransomware and Internet of Things: A new security nightmare, in: 2019 9th International Conference on Cloud Computing, Data Science Engineering, Confluence, 2019, pp. 551–555, http://dx.doi.org/10.1109/CONFLUENCE.2019.8776926.

[128] Ibrar Yaqoob, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, Mohsen Guizani, The rise of ransomware and emerging security challenges in the Internet of Things, Comput. Netw. 129 (2017) 444–458.

[129] J. Deogirikar, A. Vidhate, Security attacks in IoT: A survey, in: 2017 International Conference on I-SMAC, IoT in Social, Mobile, Analytics and Cloud, I-SMAC, 2017, pp. 32–37, http://dx.doi.org/10.1109/I-SMAC.2017.8058363.

[130] Nicolas Falliere, Liam O. Murchu, Eric Chien, W32. stuxnet dossier, 5(6), White paper, Symantec Corp, 2011, p. 29, Security Response.

[131] Sam Edwards, Ioannis Profetis, Hajime: Analysis of a decentralized internet worm for IoT devices, Rapidity Netw. 16 (2016).

[132] Evan Cooke, Farnam Jahanian, Danny McPherson, The zombie roundup: Understanding, detecting, and disrupting botnets, SRUTI 5 (2005) 6.

[133] Elisa Bertino, Nayeem Islam, Botnets and Internet of Things security, Computer (2) (2017) 76–79.

[134] Georgios Kambourakis, Constantinos Kolias, Angelos Stavrou, The mirai botnet and the iot zombie armies, in: MILCOM 2017-2017 IEEE Military Communications Conference, MILCOM, IEEE, 2017, pp. 267–272.

[135] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna, Your botnet is my botnet: analysis of a botnet takeover, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, ACM, 2009, pp. 635–647.

[136] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, Jeffrey Voas, DDoS in the IoT: Mirai and other botnets, Computer 50 (7) (2017) 80–84.

[137] Dmitri Alperovitch, et al., Revealed: Operation Shady RAT, volume 3, McAfee, 2011.

[138] Jelena Milosevic, Nicolas Sklavos, Konstantina Koutsikou, Malware in IoT Software and Hardware, 2016.

[139] Gilles Piret, Jean-Jacques Quisquater, A differential fault attack technique against SPN structures, with application to the AES and KHAZAD, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2003, pp. 77–88.

[140] Jean-Francois Dhem, Francois Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, Jean-Louis Willems, A practical implementation of the timing attack, in: International Conference on Smart Card Research and Advanced Applications, Springer, 1998, pp. 167–182.

[141] David Mills, et al., Network Time Protocol, Tech. Rep., RFC 958, M/A-COM Linkabit, 1985.

[142] David D. Clark, Scott Shenker, Lixia Zhang, Supporting real-time applications in an integrated services packet network: Architecture and mechanism, in: ACM SIGCOMM Computer Communication Review, volume 22, (4) ACM, 1992, pp. 14–26.

[143] Hassan N. Noura, Ola Salman, Ali Chehab, Raphaël Couturier, DistLog: A distributed logging scheme for IoT forensics, Ad Hoc Netw. (2019) 102061.

[144] Mandy Douglas, Karen Bailey, Mark Leeney, Kevin Curran, An overview of steganography techniques applied to the protection of biometric data, Multimedia Tools Appl. 77 (13) (2018) 17333–17373.

[145] John D. Woodward Jr., Christopher Horn, Julius Gatune, Aryn Thomas, Biometrics: A Look At Facial Recognition, Technical report, RAND CORP SANTA MONICA CA, 2003.

[146] Anil K. Jain, Arun Ross, Salil Prabhakar, An introduction to biometric recognition, IEEE Trans. Circuits Syst. Video Technol. 14 (1) (2004) 4–20.

[147] Jossy P. George, Development of Efficient Biometric Recognition Algorithms Based on Fingerprint and Face (Ph.D. thesis), Christ University, 2012.

[148] Muzhir Shaban Al-Ani, Maha Abd Rajab, Biometrics hand geometry using discrete cosine transform (DCT), Sci. Technol. 3 (4) (2013) 112–117.

[149] Anil K. Jain, Ajay Kumar, Biometric recognition: an overview, in: Second Generation Biometrics: The Ethical, Legal and Social Context, Springer, 2012, pp. 49–79.

[150] K. Venkatasubramanian, S.K.S. Gupta, Security solutions for pervasive healthcare, in: Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, 2007.

[151] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, Bo Luo, Cyber-physical systems security—A survey, IEEE Internet Things J. 4 (6) (2017) 1802–1831.

[152] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel, Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses, in: Security and Privacy, 2008. SP 2008. IEEE Symposium on, IEEE, 2008, pp. 129–142.

[153] Robert M. Seepers, Jos H. Weber, Zekeriya Erkin, Ioannis Sourdis, Christos Strydis, Secure key-exchange protocol for implants using heartbeats, in: Proceedings of the ACM International Conference on Computing Frontiers, ACM, 2016, pp. 119–126.

[154] Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, Sok: Security and privacy in implantable medical devices and body area networks, in: 2014 IEEE Symposium on Security and Privacy, SP, IEEE, 2014, pp. 524–539.

[155] Z. Esat Ankaralı, A. Fatih Demir, Marwa Qaraqe, Qammer H. Abbasi, Erchin Serpedin, Huseyin Arslan, Richard D. Gitlin, Physical layer security for wireless implantable medical devices, in: Computer Aided Modelling and Design of Communication Links and Networks, CAMAD, 2015 IEEE 20th International Workshop on, IEEE, 2015, pp. 144–147.

[156] Daojing He, Yi Gao, Sammy Chan, Chun Chen, Jiajun Bu, An enhanced two-factor user authentication scheme in wireless sensor networks, Ad Hoc Sens. Wirel. Netw. 10 (4) (2010) 361–371.

[157] Hsiu-Lien Yeh, Tien-Ho Chen, Pin-Chuan Liu, Tai-Hoo Kim, Hsin-Wen Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 11 (5) (2011) 4767–4779.

[158] Ding Wang, Wenting Li, Ping Wang, Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inf. (2018).

[159] Tien-Ho Chen, Wei-Kuan Shih, A robust mutual authentication protocol for wireless sensor networks, ETRI J. 32 (5) (2010) 704–712.

[160] Jiye Kim, Donghoon Lee, Woongryul Jeon, Youngsook Lee, Dongho Won, Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks, Sensors 14 (4) (2014) 6443–6462.

[161] Chun-Ta Li, Chi-Yao Weng, Cheng-Chi Lee, An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks, Sensors 13 (8) (2013) 9589–9603.

[162] Prosanta Gope, Tzonelih Hwang, et al., A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks, IEEE Trans. Ind. Electron. 63 (11) (2016) 7124–7132.

[163] Pardeep Kumar, Amlan Jyoti Choudhury, Mangal Sain, Sang-Gon Lee, Hoon-Jae Lee, RUASN: a robust user authentication framework for wireless sensor networks, Sensors 11 (5) (2011) 5020–5046.

[164] Sejong Oh, Seog Park, Task–role-based access control model, Inf. Syst. 28 (6) (2003) 533–562.

[165] Peng Wang, Lingyun Jiang, Task-role-based access control model in smart health-care system, in: MATEC Web of Conferences, volume 22, EDP Sciences, 2015, p. 01011.

[166] Indrakshi Ray, Manachai Toahchoodee, A spatio-temporal role-based access control model, in: IFIP Annual Conference on Data and Applications Security and Privacy, Springer, 2007, pp. 211–226.

[167] S. Muthurajkumar, M. Vijayalakshmi, A. Kannan, Intelligent temporal role based access control for data storage in cloud database, in: Advanced Computing, ICoAC, 2014 Sixth International Conference on, IEEE, 2014, pp. 184–188.

[168] James B.D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, A generalized temporal role-based access control model, IEEE Trans. Knowl. Data Eng. 17 (1) (2005) 4–23.

[169] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, Channel surfing and spatial retreats: defenses against wireless denial of service, in: Proceedings of the 3rd ACM Workshop on Wireless Security, ACM, 2004, pp. 80–89.

[170] Tongbo Luo, Zhaoyan Xu, Xing Jin, Yanhui Jia, Xin Ouyang, Iotcandyjar: Towards an Intelligent-Interaction Honeypot for Iot Devices, Black Hat, 2017.

[171] Quang Duy La, Tony Q.S. Quek, Jemin Lee, A game theoretic model for enabling honeypots in IoT networks, in: Communications, ICC, 2016 IEEE International Conference on, IEEE, 2016, pp. 1–6.

[172] Seamus Dowling, Michael Schukat, Hugh Melvin, A zigbee honeypot to assess IoT cyberattack behaviour, in: Signals and Systems Conference, ISSC, 2017 28th Irish, IEEE, 2017, pp. 1–6.

[173] M. Anirudh, S. Arul Thileeban, Daniel Jeswin Nallathambi, Use of honeypots for mitigating DoS attacks targeted on IoT networks, in: Computer, Communication and Signal Processing, ICCCSP, 2017 International Conference on, IEEE, 2017, pp. 1–4.

[174] R. Melki, H.N. Noura, M.M. Mansour, A. Chehab, An efficient OFDM-based encryption scheme using a dynamic key approach, IEEE Internet Things J. (2018) 1, http://dx.doi.org/10.1109/JIOT.2018.2846578.

[175] H. Noura, R. Couturier, C. Pham, A. Chehab, Lightweight stream cipher scheme for resource-constrained IoT devices, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob, 2019, pp. 1–8, http://dx.doi.org/10.1109/WiMOB.2019.8923144.

[176] Hassan Noura, Ali Chehab, Raphael Couturier, Lightweight dynamic key-dependent and flexible cipher scheme for IoT devices, in: 2019 IEEE Wireless Communications and Networking Conference, WCNC, IEEE, 2019, pp. 1–8.

[177] Hassan Noura, Ali Chehab, Mohamad Noura, Raphaël Couturier, Mohammad M. Mansour, Lightweight, dynamic and efficient image encryption scheme, Multimedia Tools Appl. 78 (12) (2019) 16527–16561.

[178] Hassan N. Noura, Ali Chehab, Raphael Couturier, Efficient & secure cipher scheme with dynamic key-dependent mode of operation, Signal Process., Image Commun. 78 (2019) 448–464.

[179] Hassan Noura, Ali Chehab, Lama Sleem, Mohamad Noura, Raphaël Couturier, Mohammad M. Mansour, One round cipher algorithm for multimedia IoT devices, Multimedia Tools Appl. (2018) 1–31.

[180] Hassan N. Noura, Reem Melki, Ali Chehab, Mohammad M. Mansour, A physical encryption scheme for low-power wireless M2M devices: a dynamic key approach, Mob. Netw. Appl. 24 (2) (2019) 447–463.

[181] Hassan Noura, Lama Sleem, Mohamad Noura, Mohammad M. Mansour, Ali Chehab, Raphaël Couturier, A new efficient lightweight and secure image cipher scheme, Multimedia Tools Appl. 77 (12) (2018) 15457–15484.

[182] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, Lei Shu, Authentication protocols for Internet of Things: a comprehensive survey, Secur. Commun. Netw. 2017 (2017).

[183] Hassan Noura, Ola Salman, Ali Chehab, Raphael Couturier, Preserving data security in distributed fog computing, Ad Hoc Netw. 94 (2019) 101937.

Jean Paul Yaacoub is a master student in Cyber Security and Digital Forensics in the department of Electrical and Computer Engineering of (AUB), Lebanon.

Mohamad Noura is a Ph.D. student in computer science in University Bourgogne Franche Comté, France.

Hassan Noura is a research associate in the department of Electrical and Computer Engineering of (AUB), Lebanon.

Ola Salman is a Ph.D. student in the department of Electrical and Computer Engineering of (AUB), Lebanon.

Elias Yaacoub is an associate professor in the department of Computer Science and Engineering Department, Qatar University, Doha, Qatar.

Raphaël Couturier is a professor in computer science in University Bourgogne Franche Comté (UBFC), France.

Ali Chehab is a professor in the department of Electrical and Computer Engineering of the American University of Beyrouth (AUB), Lebanon.