ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Cybersecurity for the Internet of Medical Things (IoMT)

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΑΠΟΣΤΟΛΙΔΟΥ ΑΝΑΣΤΑΣΙΑΣ-ΓΕΩΡΓΙΑΣ

Επιβλέπων : Περικλής Χατζημίσιος
Καθηγητής, Διεθνές Πανεπιστήμιο της Ελλάδος

Θεσσαλονίκη, Οκτώβριος 2022

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Cybersecurity for the Internet of Medical Things (IoMT)

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΑΝΑΣΤΑΣΙΑΣ-ΓΕΩΡΓΙΑΣ ΑΠΟΣΤΟΛΙΔΟΥ

Επιβλέπων : Περικλής Χατζημίσιος
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις 1 Οκτωβρίου 2022.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Περικλής Χατζημίσιος Καθηγητής ΔΙ.ΠΑ.Ε.	Κωνσταντίνος Γουλιάνας Αναπληρωτής Καθηγητής ΔΙ.ΠΑ.Ε.	Κωνσταντίνος Διαμαντάρας Καθηγητής ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Οκτώβριος 2022

(Υπογραφή)

.....

ΑΝΑΣΤΑΣΙΑ-ΓΕΩΡΓΙΑ ΑΠΟΣΤΟΛΙΔΟΥ

Απόφοιτος Τμήματος Εφαρμοσμένης Πληροφορικής – Πανεπιστήμιο Μακεδονίας

© 2022– All rights reserved

Περίληψη

Το Διαδίκτυο των Ιατρικών Πραγμάτων (Internet of Medical Things - IoMT) αποτελεί μία υποκατηγορία του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) που επιτρέπει στο ιατρικό προσωπικό να αναλύει σε πραγματικό χρόνο εξ' αποστάσεως τα δεδομένα που λαμβάνονται από αισθητήρες που είναι συνδεδεμένοι με τον ασθενή. Ο στόχος των συσκευών IoMT είναι να παρακολουθούν συνεχώς την υγεία του ασθενή και να εντοπίσουν πιθανά ζητήματα σε πρώιμο στάδιο. Ωστόσο, η χρήση ασύρματων πρωτοκόλλων επικοινωνίας για την ανταλλαγή δεδομένων δημιουργεί κενά ασφαλείας και κάνει τις συσκευές ευάλωτες, ενώ το γεγονός ότι μιλάμε για ευαίσθητα προσωπικά δεδομένα μπορεί να αποτελέσει πόλο έλξης για κυβερνοεπιθέσεις. Οι συνήθεις τεχνικές ασφαλείας δεν μπορούν να χρησιμοποιηθούν, καθότι οι συσκευές IoMT διαθέτουν περιορισμένη ισχύ και υπολογιστική δύναμη. Σε αυτό το πλαίσιο πραγματοποιήσαμε μία εκτεταμένη έρευνα για τις ταξινομίες στην κυβερνοασφάλεια, ώστε να μπορέσουμε να τις συγκρίνουμε και να εντοπίσουμε πού μπορούμε να συνεισφέρουμε. Κύριο ενδιαφέρον μας είναι το IoMT, το οποίο αντιμετωπίζει παρόμοια ζητήματα ασφαλείας όπως το IoT, αλλά είναι ακόμα πιο σημαντικό να προασπίσουμε την ασφάλειά του λόγω της φύσης των δεδομένων. Παρουσιάζουμε μία ταξινομία, λοιπόν, αναφορικά με την κυβερνοασφάλεια του IoMT με μία σφαιρική προσέγγιση, εξετάζοντας τις απειλές, προσδιορίζοντας τα κίνητρα πίσω από μία επίθεση, την ίδια την επίθεση, τις ικανότητες του επιτιθέμενου, τον αντίκτυπο και τα αντίμετρα. Η ταξινομία αυτή μπορεί να χρησιμοποιηθεί είτε για αντιμετώπιση επίθεσης, είτε προληπτικά. Κλείνουμε παρουσιάζοντας προκλήσεις στον κλάδο, που μπορούν να χρησιμεύσουν ως κατεύθυνση για μελλοντική μελέτη.

Λέξεις Κλειδιά: Cybersecurity, Taxonomies, Internet of Medical Things, Internet of Things

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

The Internet of Medical Things (IoMT) is an application of the Internet of Things (IoT) that enables medical personnel to remotely analyze physiological data obtained from patient-associated sensors. The goal of IoMT devices is to continuously monitor a patient's health and identify potential issues at an early stage. However, using wireless connection for data transfer leaves this data vulnerable to cyberattacks, and the fact that this data is private and sensitive may be an attraction pole to attackers. Traditional security techniques are useless when used on hardware with constrained storage and processing power, resources like IoMT devices offer. In this context, we have performed a comprehensive survey for cybersecurity taxonomies, so we can compare them and determine where we can contribute. Our primary area of interest is the IoMT, which encounters similar impediments in cybersecurity as IoT, but it is even more critical to secure due to the nature of the data. We present a taxonomy for IoMT cybersecurity in a holistic dimension. We review the various threats that can affect IoMT and identify the motives behind an attack, the attack itself, attacker's capabilities, the impact and countermeasures. The recommended taxonomy can be used either for attack mitigation or preventively. Then we discuss some challenges, which can serve as direction for future study.

Keywords: Cybersecurity, Taxonomies, Internet of Medical Things, Internet of Things

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1

Introduction

1.1 IoMT as part of IoT

A wide range of entities, including people, machines, and objects, are connected into the information space anywhere at any time under the Internet of Things (IoT) umbrella. IoT plays a significant part by providing streamlined and seamless ubiquitous services for everyone, which reduces manual labor and helps to connect everyone to almost anything [202]. The IoT is a broad term for the networking of physical objects that are intelligent and networked [79] and includes sensors, software, and network connectivity that enables it to collect and exchange data. As it makes its way into every international company and consumer domain, the IoT is currently reshaping and revolutionizing both the commercial and consumer worlds. In addition to this, it is being provided in a wide range of other fields, such as healthcare, smart cities, agriculture, the military, and so forth [79,80,203,204,205]. Consequently, the IoT may greatly improve how people engage with the outside world. According to recent projections, the IoT market size is expected to reach USD 1386.06 billion by 2026, demonstrating its significance as a leading technological paradigm for enhancing the well-being of billions of people around the globe [19,206,207,208].

The Internet of Medical Things (IoMT), in which medical devices are connected in a worldwide network that anyone, anywhere, and at any time may have access to, is a result of the development and growth of IoT and is revolutionizing the healthcare sector. In terms of health services, IoMT-based applications have taken a stunning lead, inspiring millions of people

worldwide to lead healthier lives. With the aid of IoMT devices, the health of patients can be monitored remotely and in real-time, like a 24/7 healthcare provider, with exact, widespread and customized services.

A typical IoMT healthcare system, in general, consists of a number of medical equipment embedded with different types of intelligent sensors that can sense their environment [209,210]. The medical data can be analyzed by a smart device or on the cloud, where a wireless medium is utilized to provide the medical data to stakeholders, like doctors or nurses, assisting them in making decisions regarding the patient's condition [15,207,210,211,212]. These intelligent devices can also be connected to global information networks for easy, on-demand access. The ability to remotely access devices designed for the monitoring, analysis, forecasting, and storage of critical medical data is made possible by the integration and connectivity of physical objects in the IoMT environment to the Internet [213,214]. So, it is a fact that the IoT has altered the healthcare industry, allowing healthcare providers to provide their services to clients at home, where they may remotely monitor, track, and treat clients' illnesses while they go about their daily lives. However, some issues that are quickly approaching call for urgent attention in order to be addressed if we are to get the most out of these healthcare applications through IoMT. The privacy and safety of patients are particularly in danger from IoMT devices, such as medical wearable and implanted sensors, which make up the essential underlying components of the IoMT edge network.

With the rapid expansion of IoMT devices, private patient data is made available to third parties and is easily accessible in a variety of ways. For instance, a hacker may intercept data being sent over the wireless network and eavesdrop through the network to get private patient information. In the worst-case circumstances, attacker could gain remote access to the medical device's control unit and use it to manipulate it, endangering the lives of patients [5,214]. Furthermore, it would be a serious risk to the patient's privacy if a passive network observer could infer sensitive patient data from the network traffic, especially if the information inferred might later be misused [215,216]. It is clear that the end-users and other relevant stakeholders (such as medical staff, patients, and caregivers) lack sufficient knowledge about IoMT security, which may exacerbate vulnerabilities and encourage attackers to further exploit IoMT technologies, endangering patients' lives in the majority of cases [19,80,205,207]. Recent trends show that the healthcare IoT security market is anticipated to experience rapid growth by the year 2025, with a total revenue of USD 100 billion, which also justifies our efforts to examine the current state of security and privacy of the IoMT through this study [215-218].

So, we have conducted a deep survey on cybersecurity taxonomies in general and in IoMT in particular. Our review focuses both on the current and potential security risks to the IoMT edge network environment and we provide a classification based on the main security objectives that

these threats target. Additionally, we consider attacker's motivation and compromised layers to detect the attack method, so we can also include in our taxonomy the impact and damage range and some countermeasures to mitigate similar attacks in the future.

1.2 Motivation

In November of 2019, COVID-19, a fatal virus outbreak, suddenly appeared over the planet, posing a threat to everyone. Given the current level of accessible medical resources, the virus has caused the global population to drop by about 6.5 million people as of the time that we are writing thesis [201]. This raises serious concerns about how to control the pandemic going forward. In order to restrict and contain the spread of the virus, lockdowns have been implemented throughout the world, including statewide and national lockdowns. Due to the spreading nature of the virus and to lessen the burden on the healthcare facilities, some governments assisted in the introduction of a number of IoMT-based technologies to track and treat patients remotely. According to recent studies [217-221], this increased demand for devices and technology during the pandemic season has also increased the number of IoMT security assaults, which further inspired us to put together the study.

While many academics and suppliers are presently striving to strengthen the security and privacy aspects of the IoMT ecosystem, the use of IoMT in healthcare is expanding quickly as a result of recent demand, making it impossible to solve all security and privacy concerns in a timely manner. However, the IoMT concept itself is a unique idea, and research in terms of security and privacy is still in its infancy. Our goal in conducting this study was to ascertain the current state of knowledge regarding the security and privacy aspects of IoMT, compile it, and create opportunities for future research that would be extremely helpful for academics, vendors, and researchers interested in the security and privacy aspects of IoMT.

1.3 Contribution

There have been rapid contributions in the area of cybersecurity taxonomies in general, proposing novel solutions for risk assessment purposes mostly. There is a significant number of research studies and surveys being provided on the topic.

However, when it comes to cybersecurity taxonomies in the IoMT domain, a few surveys have also been conducted on the topic in general, where it is not able to provide a holistic knowledge to conduct future research and to devise sound security solutions towards improving the security and privacy of the pervasive IoMT environment. This study offers an in-depth overview of the cybersecurity aspects of IoMT in order to fill the research vacuum by outlining its ecosystem,

important contributions, most recent trends, countermeasures and solutions, difficulties, and future directions. Our contributions are summarized as follows:

- We provide adequate knowledge about IoT and IoMT ecosystem and highlight their cybersecurity aspects and demands.
- We provide a brief comparison of the existing literature, highlighting its key contributions and limitations to justify our work and better understand what is trending now.
- We classify IoMT in cybersecurity aspects, examining the attack itself, motivation, the attacker, communication protocols leaked, compromise level, impact, damage range and suggest countermeasures and solutions to prevent attacks in the future.
- We discuss possible expansion in the future of the taxonomy we suggested and other aspects of cybersecurity in IoMT for further research.

1.4 Methodology

We have made comprehensive research in IEEE, Google Scholar, ENISA and NIST for papers that included surveys on cybersecurity taxonomies, or they referred to taxonomies. Then, in order to provide more information in IoMT domain, we searched for papers which included 'IoMT' or offered IoMT taxonomies.

1.5 Outline of study

In order to provide a comprehensive review, as stated in Section 1.2, the rest of the paper is organized as follows: In Section 2, we discuss the background in IoT and IoMT cybersecurity, providing and comparing related work and contributions made by others. In Section 3, we present our proposed cybersecurity taxonomy for IoMT. In Section 4, we suggest future directions and open a discussion for further expansion of our research. Finally, the conclusions are presented in Section 5.

2

Background

2.1 IoT

The IoT and its related technologies can be used in a wide range of industries, but connected things are always linked to the same kind of architecture because they require data to be transferred, stored, processed, and made available.

The authors of [189] described a general, four-level architecture for the Internet of Things. Wireless links or wired technologies (such as Ethernet, fiber optics, etc.) are used by these components to communicate (Bluetooth Low Energy, Wi-Fi, ZigBee, etc.) [190]. The optional local pickup places may include smartphones, minicomputers, and other items. They serve as entrance points for weaker things to access the infrastructure (battery, computing power, etc.). They occasionally permit close contact between the user and the objects (an application on a smartphone for example).

The transport level enables communication between the local pickup locations or objects and the command servers. The processing of the data is made possible by the cloud-based storage and data mining. Finally, the data can be accessed by the user or other systems using APIs or GUIs. Only the first level -the local environment- is unique to the Internet of Things; the other three are present whenever sizable amounts of data are processed.

A definition for a connected object could be: "Sensor(s) and/or actuator(s) carrying out a defined function and that are able to communicate with other equipment" [150]. This description takes into account the previous components. It is a component of the infrastructure that enables users or other systems to access, transport, store, process, and use the created data. The Internet of Things would then be described as a "group of infrastructures interconnecting connected items and enabling their management, data mining, and access to the data they generate".

2.2 IoMT

IoMT is essentially an IoT-based solution that enables the creation of IoT-enabled healthcare systems for the observation of numerous various types of vital signs, including electrocardiogram (ECG), heart rate, and blood pressure [182]. The primary goal of IoMT-enabled healthcare systems is to raise patients' quality of life by reducing the likelihood of an uncomfortable hospital stay [186]. A key component of high-quality medical service delivery is allowing patients to move freely throughout both medical and non-medical settings while also ensuring uninterrupted continuous monitoring of their vital signs and health condition [183-185].

The IoMT edge network is the key element of an IoMT-based healthcare system. It consists of a wide range of IoMT-capable devices that allow people to track their physical wellness and monitor their health status digitally [187, 188]. For instance, the users can access their health information from any computer or mobile device at any time. IoMT-enabled devices can include a variety of sensors including ECG sensors, electroencephalography (EEG) sensors, airflow sensors, blood pressure sensors, motion sensors, and activity sensors. It is important to highlight that IoMT-enabled sensors have ubiquity and widespread identification, sensing, and communication capabilities, enabling the collection of vital signs from any location (such as a home, hospital, or office) [183]. Additionally, the user's terminal device (such as a smartphone) that serves as the smart e-health gateway is a part of the IoMT edge network. Depending on the network's availability, this gateway is in charge of receiving and transmitting the vital sign data to either (i) a cellular base station using long-range wireless technologies (such as 4G/5G) or (ii) a router using short coverage communication protocols., such as Bluetooth and 6LoWPAN, or Wi-Fi, so that the vital sign data will reach, over the Internet, the Cloud platform services at the healthcare provider side for further data processing and storage [182, 183]. The gathered health data can serve as a big data source for statistical and epidemiological studies. Patients can access cloud services at any time and from any location. Likewise, licensed healthcare practitioners have access to these services in order to diagnose and treat people medically.

2.2.1 IoMT Communications

There are four primary communication network types that are used for real-time data transmission between medical equipment: Body Area Networks, Home Area Networks, Neighborhood Area Networks, and Wide Area Networks are a few examples of these sorts [21].

- Body Area Network (BAN): A BAN is a network channel for transmitting patients' vital signals, which are determined by a wearable or portable sensor. According to [75], biological signals can be used to protect medical device connections. In order to secure the connection

between BAN sensors, [129] introduced a low-power bio-identification technique. They did this by using an Inter-Pulse Interval (IPI). The authors of [164] were able to employ a physiological signal for BAN sensor communications that is in agreement with the secret key of the symmetric key cryptosystem. As a result, there are two methods that the controller receives the medical data collection: Smartphone: transfers the gathered data to the base station (BS), which then routes it till it gets to the medical data center, using a mobile network. Using one of the several wireless communication protocols, such as Zigbee, Bluetooth, or Wi-Fi, a wireless medical device delivers data.

- Home Area Network (HAN): A HAN makes use of a controller to handle communication as the data is sent to an accessible Access Point (AP) in the patient's home. Wi-Fi or LTE can be used for transmissions [42].
- Neighborhood Area Network (NAN): A NAN enables users to connect to the Internet fast [175]. It is employed to create wireless connections between nearby regions, such as neighborhoods and homes. A single AP can span a radius of at least half a mile using an omnidirectional antenna as its foundation. A directional antenna can also be used by a NAN to boost the AP's signal.
- Wide Area Network (WAN): The communication from a mobile base station or an access point to the mobile/Internet (remote) medical infrastructure is represented by a WAN. A WAN guarantees real-time data delivery to emergency response teams in times of need. The AP can also deliver the data to cloud services after it has been received so that it can be stored at the designated server.

2.2.2 IoMT devices

Depending on the patient's needs, numerous medical devices are available. In reality, a lot of them are being employed by hospitals for real-time smart remote monitoring or are offered as gadgets on the medical market. Fitness trackers, blood pressure monitors, and sugar level monitors are some examples of these smart medical equipment.

A considerably more advanced and appropriate health-care system is required due to the expanding elderly population in wealthy nations. IoMT ensures patients' physical mobility, which reduces the number of patients in hospitals undergoing Blood Pressure (BP) or CardioVascular Disease (CVD) examinations, which, according to the World Health Organization (WHO), account for 30% of all fatalities worldwide. In addition, hospitals can now remotely monitor diabetes cases. These gadgets can be carried, worn, or implanted. Plus, while some gadgets are specialized and meant to be used in hospitals and clinics, others can be used at home.

- Wearable and Personal Devices: Smart and electronic medical gadgets that collect, monitor, and improve patients' health problems in real-time and at a lower cost are included in the category of wearable and personal devices [169]. Fitness trackers, smart health watches, wearable Blood Pressure Monitors (BPM), ring-style heart rate monitors, and biosensors are examples of wearable technology [78]. There is an even greater need for tele-home healthcare as a result of the aging population and the growth of diseases. Examples of wearable of personal devices are listed below:
    - Smart Fitness Devices: They help people maintain healthy lifestyles and enhance their physical well-being. This is accomplished by establishing a daily exercise schedule that varies and is based on the patient's condition, age, gender, physical condition, and capacity.
    - Smart Blood-Pressure Devices: They are used throughout a wide range of IoMT disciplines and domains. They are utilized to remotely and continuously check patients' blood pressure. These devices monitor blood pressure variations in an effort to quickly identify any anomalies and communicate the data in real-time.
    - Smart Glucose-Level Devices: They are used to track and monitor the blood sugar levels of people with diabetes types I and II. They assist in preserving the proper insulin level to safeguard the patients. This lessens the effects and dangers of unexpectedly increased or lower insulin levels. Signals are transmitted to the insulin pump's actuators to administer the right amount of insulin in the event of an insulin decrease. The spinal cord stimulator, which is implanted in the patient's body to provide long-term pain treatment, is another example of an actuator [79].
    - Smart Heart-Rate Devices: They can save patients' lives and are employed in many different medical fields. While conventional devices only provide urgent data when an anomaly is discovered, a group of devices can continuously monitor the heart rates of individuals. As a result, the primary function of these gadgets is to foresee potential heart attacks before they happen. These gadgets could consist of various heart-rate monitors, wearable wireless sensor networks, and BANs.
    - Smart Diet Devices: They are used to help patients, who primarily struggle with eating problems, maintain a balanced diet. Those devices are specifically used by overweight persons who have trouble adhering to a diet or occasionally forget about its restrictions. In reality, digital diet tools have replaced printed diet plans on paper. These gadgets can automatically update users' regular diets with various nutrition ingredients, via a smart diet software [92].

Except for wearable and personal devices, there are more IoMT devices listed below.

- In-home Medical Devices: These include ventilators, infusion pumps, and dialysis units that are currently utilized outside of a hospital or clinic, are also supplied by a healthcare provider, and connect with the hospital via basic technologies (e-mail, the Internet, smart medical devices) [60]. Among these devices there are test kits, first aid gear, durable medical gear, feeding gear, urination gear, treatment gear, respiratory gear, baby gear, and other gear among them [37].
- In-Hospitals and Clinics Medical Devices: Regardless of whether an incident or emergency is life threatening, hospitals must always be ready. Because of this, providing patients with the proper care requires a high degree of readiness from both medical professionals and equipment. Medical donations are essential in this situation [125]. Defibrillators, anesthetic machines, patient monitors, ECG Machines [2], surgical tables, blanket and fluid warmers, electro-surgical units, surgical tables, and lighting are a few examples of such medical equipment [1].

2.2.3 IoMT cybersecurity concerns

2.2.3.1 Security concerns

IoMT devices are vulnerable to a variety of wireless/network assaults since they depend on the use of open wireless connections. In fact, a skilled attacker may quickly get beyond inadequate security authentication procedures on most IoMT devices, allowing them to listen in on and intercept incoming and outgoing data and information. Due to the inability to recognize and stop such attacks, it is also possible to get illegal access without being noticed. This could lead to higher privileges, the injection of malicious code, or the malware infection of devices.

IoMT devices could be hijacked (as botnets) and employed to carry out Distributed Denial of Service (DDoS) assaults. Medical devices are vulnerable to botnet or "zombie" attacks, which can result in physical assaults on patients, as mentioned in [32]. For instance, an attack may rationally modify a drug dose that would kill the target patient or have severe health effects. Additionally, when taken over by terrorists, IoMT devices could be utilized as a tool for targeted assassination. In order to prevent being hacked in order to kill him, US Vice President Dick Cheney turned off the wireless functioning of his heart implant [126]. Additionally, as stated in [32], IoMT devices can negatively impact patients' psychological well-being since they may frighten them and cause them to experience a heart attack as a result of being surrounded by machines rather than people.

To guarantee and maintain the security of the IoMT devices along with medical systems and devices alike, manufacturers of medical equipment must prioritize security as a highest concern.

To reduce the main IoMT security issues, protection against passive and active attacks is necessary. Consequently, it is essential to use the appropriate security tools and techniques.

2.2.3.2 Privacy concerns

Due to the possibility of gathering and disclosing patient identities together with sensitive and confidential information, passive attacks like traffic analysis raise privacy concerns. The ability of an attacker to identify a patient's medical information and illnesses poses a grave threat to the patient's life, making this a very significant threat. Identity theft is another way why patients' privacy is violated when hospitals are attacked. In the majority of these real-life attacks, personal or sensitive information was leaked or otherwise disclosed, resulting in a breach of patients' privacy. In conclusion, maintaining the confidentiality of private and sensitive medical information is only one aspect of privacy. Additionally, it calls for the requirements of non-observability, non-linkability, and anonymity [21].

- Non-observability: Non-observability is the state of Items Of Interest (IoI) being indistinguishable from any IoI of the same type. This implies that messages cannot be separated from random noise (s). In other words, whether a communication has been sent or received by a sender/receiver in a relationship should not be obvious.
- Non-linkability: Passive attacks should not reveal Items of Interest (IoI), such as subjects, messages, events, or activities. This implies that the likelihood of those objects remaining hidden from the attacker's perspective both before and after observation should be the same.
- Anonymity: When a patient is communicating, his identity should be concealed so that he cannot be identified. In other words, passive assaults only have access to your actions and not your identity.

2.2.3.3 IoMT risks and challenges

- Trust issues: Patients' privacy being violated can result in significant trust concerns. Patients are growing weary of the notion of robots taking over human duties (doctors, nurses, and receptionists). People are consequently more worried about having a medical robot, machine, or even device monitoring and managing their health concerns. The challenge here is to earn patients’ trust again that their data will be safe as a highest priority.
- Disclosure of personal information can seriously affect patients’ medical conditions, as well as hospital’s reputation.
- Data falsification might lead to the transmission of any medical device's data being altered and modified, which could lead to a greater drug dosage or an incorrect medical description that could cause additional medical issues, even lead to death.

- Whistle-blowers are based on disgruntled or dishonest medical staff members who risk patients' privacy and lives by divulging medical information about the hospital or patients by being bribed or participating in organized crime.
- Lack of training among nurses and doctors can result into risking patients' lives with lifelong disability or the loss of life.
- Accuracy is still a contentious topic, and it continues to be the cause of errors in the medical procedures carried out by specialized robots. Additionally, this may have a negative impact on the patients' quality of life and result in harm or death.

2.3 Cybersecurity in IoT and IoMT

It is popular to define cybersecurity as a composition of confidentiality, integrity, and availability (CIA) [191]. There are various ways to enlarge this definition. For instance, [192] categorizes information and communication technology (ICT) and cybersecurity into the following categories: Information security is the protection of information as a valuable asset in and of itself.; ICT security is defined as safeguarding the network, or more specifically, the technology-based systems used to transport and retain information. Cybersecurity also includes other non-information-based assets that are susceptible to threats from ICT, such as home automation [128].

In our paper we will use cybersecurity definition as descripted above. IoT and its subcategories face cybersecurity issues in communication protocols, such as Bluetooth, Wi-Fi etc. The differentiation of each circumstance is upon the attacker motives, the nature of the attack (e.g., internal/external) and other factors, like the capabilities of the attacker, which all together lead to the final attack method.

According to a recent study [193], 57% of IoT devices are vulnerable to attacks that reveal sensitive data because more than 90% of all IoT device traffic is unencrypted. Cyberattacks can put people's lives in danger in addition to causing systemic disruption. Any cyberattack has the potential to be catastrophic and endanger the lives of patients [194]. It may become more difficult to protect the privacy of crucial and sensitive medical data due to the rapid expansion and acceptance of IoMT, especially during pandemics. The IoMT architecture can be affected at different levels by a variety of attacks, risks, and dangers [194].

As a result, the IoMT sector is subject to stringent security and privacy regulations. Additionally, it was mentioned that the IoMT has privacy and security vulnerabilities that need to be resolved. It is advised to use techniques like cryptographic or non-cryptographic algorithms for effective intrusion detection and prevention. Data security, integrity, authenticity, and availability have all been compromised by various malware attacks on IoMT

systems. The current security strategy has prioritized key management, intrusion detection, authentication, and access control [195].

As connected cars, smart cities, and next-generation health technology develop in huge speed, hackers may choose to target these devices rather than steal private information in the virtual world [196–198]. Health information could be exposed if devices connected to the IoMT are particularly vulnerable entry points for hackers. 83% of IoT medical imaging devices are using unsupported operating systems, according to a recent survey and these devices could increase the risk of hacks that expose private medical information for healthcare organizations [193,199,200]. 98% of all IoT device communication is unencrypted, leaving 57% of IoT devices exposed to cyberattacks and exposing personal and private data on the network [193]. It should be anticipated that cyberattacks will increase in frequency and severity as well with the development of connected devices.

2.4 Literature review

2.4.1 IoT Taxonomies

The authors of [155] support that the key properties of IoT are mobility, wireless connection, embedded use, diversity and scale. Based on this, they continue with the challenges which are divided in i) management, scalability and heterogeneity of devices, ii) network knowledge and context, iii) privacy, security and trust between both the device and information exchanged. So, the high-level security requirements are among resilience to attacks, data authentication, access control, client privacy, user identification, secure storage, identity management, secure data communication, availability, secure network access, secure content, secure execution environment, tamper resistance. Their suggested threat taxonomy focuses on management issues and risk assessment, which both are significant factors in understanding the various threats associated with the use of IoT. The final scope of the taxonomy is the effective risk management, however it consists of basic characteristics of security, as it is an old publication. The taxonomy (Figure 1) classifies the threats as following:

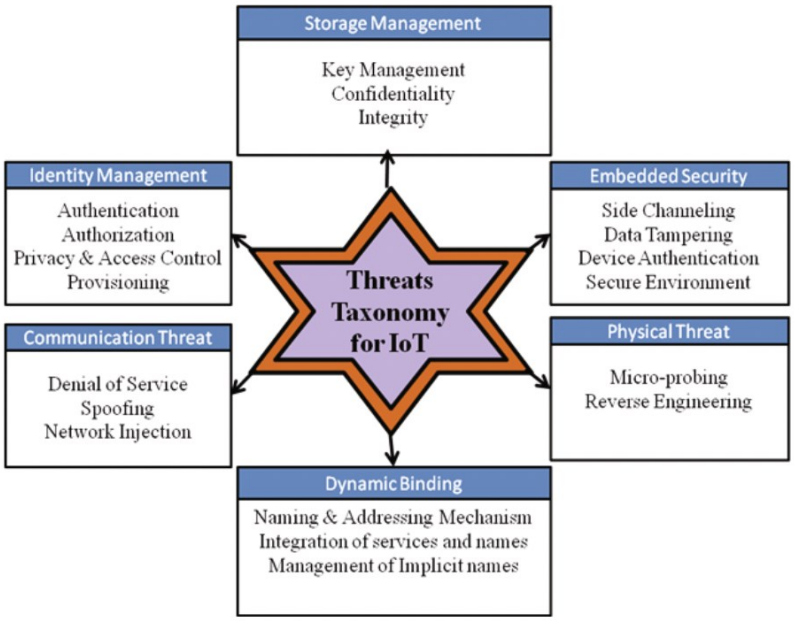

Figure 1. Threat taxonomy for the IoT [155].

Identification includes authentication, authorization, accounting, and provisioning in the determination of a unique device, user, or session. The suggestions for a safe identification in IoT are: single sign-on, identity federation, user-centric identity management and an updated and secure device.

Communication threats covers a Denial-of-Service (DoS) assault, which takes place when an attacker repeatedly spams a targeted Access Point (AP) or network with phony requests, premature success connection messages, failure messages, and/or other commands.

Physical threat includes micro probing and reverse engineering, which can seriously compromise security by altering the hardware itself. Some physical attack kinds are difficult to produce because they require pricey materials. De-packaging of chips, layout rebuilding, and micro-probing are a few examples.

Embedded Security threat model will span all dangers at the physical and MAC layers. At the device level, security threats including data and device tampering, side channel analysis, bus monitoring, etc. would be of concern.

Storage management has a significant impact on key management in order to ensure confidentiality and integrity. Choosing the right cryptographic building blocks is especially important since, for instance, the cipher texts of some public key encryption techniques may be able to reveal personal information about the intended receiver.

[150] suggests a taxonomy for connected objects (Figure 2) which revolves around the energy, communication, functional attributes, local user interface, hardware and software resources and cost.

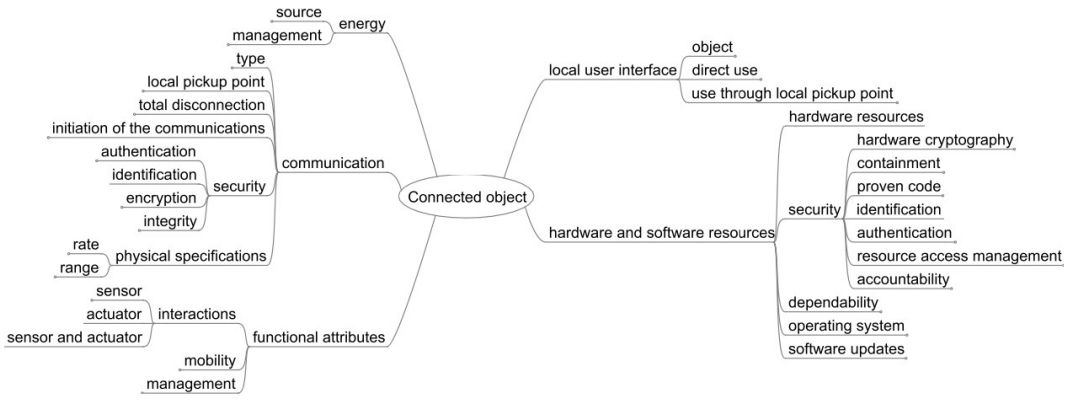

Figure 2. Taxonomy for connected objects [150].

The taxonomy proposed is indefinitely expansible, as the technology of IoT devices keeps improving. At first, they classified various connected objects, to find out that the IoT is the only in common thing in general between the connected object, as they differed in everything else: energy consumption, communication protocols, functional attributes, user interface, hardware, software, cost. So, they suggested a separation between communication security and hardware/software security and this is the differentiation of this taxonomy.

When in communication, security has authentication, identification, encryption and integrity attributes. On the other hand, hardware security depends on cryptography, containment, proven code, resource access management and accountability, as well as in authentication and identification. However, in hardware security in both authentication and identification, security relies on physically interaction between the user and the object, in contrast to communication security, where in authentication the object must recognize the user -even when not physically close enough-, either by proving both their identity or one way authentication or eventually no authentication would be required for the recognition. Plus, in identification of communication security, two objects can belong to a different group, however the communication would still be possible.

The taxonomy in [135] classifies the attacks in a subcategory of IoT according to CIAA model (confidentiality, integrity, authentication, authorization). It is a taxonomy proposed for RPL (Routing Protocol for Low power and Lossy Networks) security issues (Figure 3), with recommendations to counteract these attacks. First objective of this taxonomy is to identify and then to classify the attacks against RPL network. The advantage of the taxonomy is that the main classifier is the attacker's goal. Then, they prioritize the attack depending on the damage of the network, which is huge differentiation from other IoT taxonomies. So, it can be utilized for risk management scope.

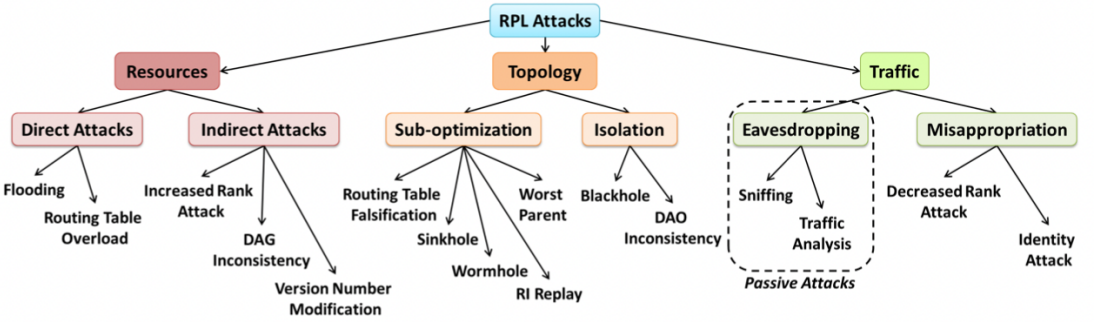

Figure 3. Taxonomy of attacks against RPL Networks [135].

The first category covers attacks targeting the exhaustion of network resources (energy, memory and power), with the main classification between direct and indirect attacks. The second category includes attacks targeting the RPL network topology. The third category corresponds to attacks against the network traffic, such as eavesdropping attacks (passive) or misappropriation attacks.

By recognizing, assessing, and managing the risks that a network or information system faces, the taxonomy can be utilized for risk management. It is also emphasized that while the attacks, their effects, and their security measures are all taken into account separately, a real attacker is likely to combine a number of these methods.

In [130] it is proposed a four-layer classification in cybersecurity of IoT devices (Figure 4), in contrast with the three-layered one in [158]. This differentiation is used to show that there are vulnerabilities in all layers: sensing, network, middleware and application. Basically, they have added as an extra the middleware, which is based in service-oriented architecture (SOA). According to the authors of [130], at this level, it is necessary to control and maintain the authenticity, integrity, and secrecy of all transferred data. By combining high spatial-temporal resolution with the pervasiveness of sensor networks and other identifiable things through the IoT architecture, intelligent middleware may create dynamic mechanisms for the physical world in the digital/virtual world. [159]. Heterogeneity of devices is considered as the no.1 factor of this classification.

[130] and [135] have 2 categories in common, talking both about access level (or resources) and information damage level as well. However, the structure and the focus of each of these taxonomies have important differences.

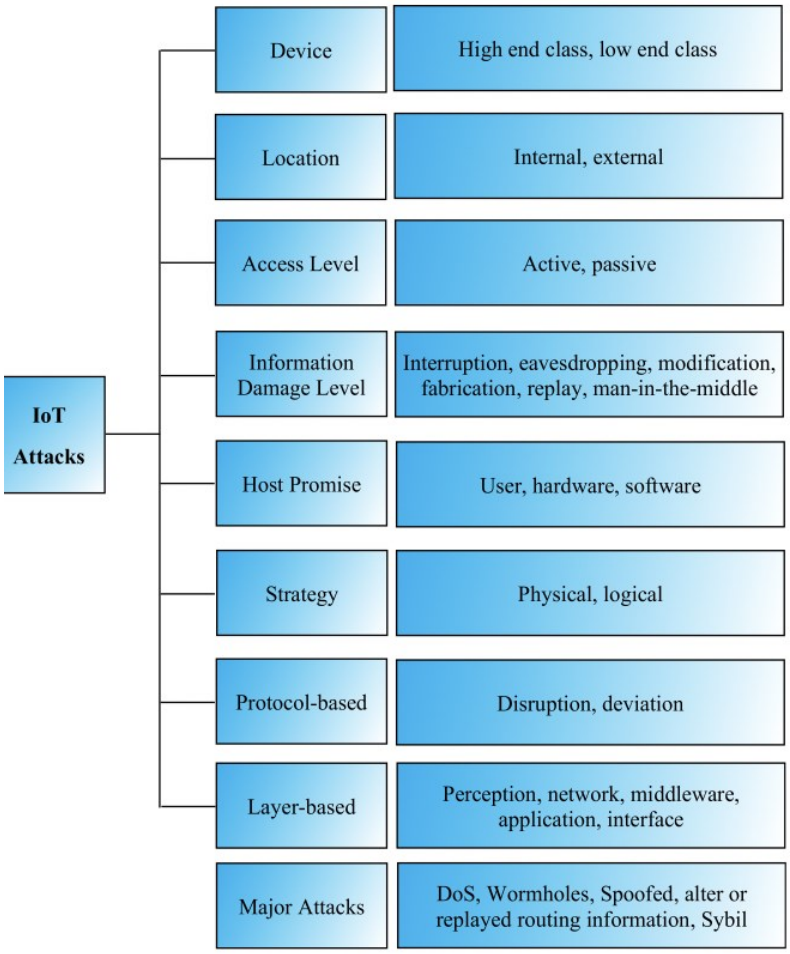

Figure 4. Taxonomy of cybersecurity attacks in IoT [130].

The taxonomy of cybersecurity attacks in IoT consists of a classification between device (regarding high-end or low-end class), internal or external location, active or passive access level, information damage level depending on the attack (eavesdropping, man-in-the-middle, modification etc), host promise (user, hardware, software), logical or physical strategy, protocol-based, layer-based and then some major attacks are mentioned separately because they have other key enabling measurements than the mentioned.

This taxonomy can be applied in healthcare service industry, smart domain, transportation and parking system. In all three domains the main goal of the taxonomy is the cybersecurity and the protection of information that could lead to illegal access or service disruption. The big advantage of the taxonomy is the lean infrastructure, however it is a very generic taxonomy.

Authors of [142] suggest an objective methodology to analyze vulnerabilities at a deeper level of granularity. The taxonomy provides an objective technique for analyzing vulnerabilities at a finer scale. Again, risk assessment management would value this taxonomy, security analysts, and network administrators of IIoT (Industrial Internet of Things) domain as well. This is a multilayer taxonomy, with 11 layers, 94 dimension and approximately 100 techniques. The

possible sequence of an attack from initial access to impact is the criteria of the classification. It is so wide that it can be used in real-world incidents, however, it has drawbacks depending on each attack, for example if a vulnerability targets the IDS itself. The main thing in common with the taxonomies in [130] and [135] is that they all include access level as a main category in the first level of the classification.

The 11 layers of this multi-layer IIoT attack taxonomy are structured as follows:

i. Initial access: consists of the methods that marketers employ to enter the IIoT environment. These methods are designed to compromise remote external services and operational technology assets.

ii. Execution: consists of attacks that give the enemy the ability to run code under their control on a local or remote system in an industrial setting. Malicious code execution may be triggered by the end user or by the performance of a specified function.

iii. Persistence: Attacks and methods used to maintain ongoing unauthorized access to the industrial environment are referred to as persistence.

iv. Evasion: Evasion is the process of keeping an enemy hidden from both technical and human defences while it is operating.

v. Discovery: Techniques used for discovery include those that are used to learn more about the industrial environment, including details on the internal network, control system components, and active processes. These methods aid adversaries in determining which networks they could take over and use for nefarious purposes.

vi. Lateral movement: Adversaries enter and take control of remote systems that are connected to the network via lateral movement tactics. These methods employ known account credentials, default credentials, and susceptible services to access the network's control systems.

vii. Collection: Attack methods for collection include acquiring system diagrams in an industrial setting or identifying the purpose of a device in order to receive contextual feedback.

viii. Command and control: Adversaries use command and control techniques to deliver unauthorized commands to controllers, devices, and systems that are compromised in the industrial setting. Human machine interfaces (HMI), servers, data historians, and engineering workstations may be among the vulnerable assets.

ix. Inhibit response function: The strategies used by advertisers to conceal input from industrial systems linked to safety, quality assurance, and operator intervention functions that react in the event of a failure, hazard, or unstable state are known as inhibit response functions.

x. Impair process control: Impair process control refers to strategies used by advertisers to undermine the logic of the control system and have a negative impact on the processes that are being monitored in the targeted industrial setting. Additionally, these strategies can include comprise the blocking of or manipulating reporting messages and control logic.

xi. Impact: Impact refers to the harm that enemies have done by destroying, disrupting, or manipulating the devices, processes, and operations of the control system.

2.4.2 Intrusion Detection System (IDS) Taxonomies

[136] intents to design an effective and efficient intrusion detection technique (Figure 5) that it is applicable to Wireless Sensor Networks (WSN). To do this, their goal is to minimize false positive rates and keep high the true positives, so this is the key factor of this taxonomy. They combine all the possible information to achieve their goal and they classify the intruder type, intrusion type, detection methodology, source of the audit area, computing location of the collected data, infrastructure, usage frequency. The only drawback of this taxonomy is that there is an amount of factors that can result more false positives out of control, for example collisions, packet drops, limited transmission power and fading battery power.

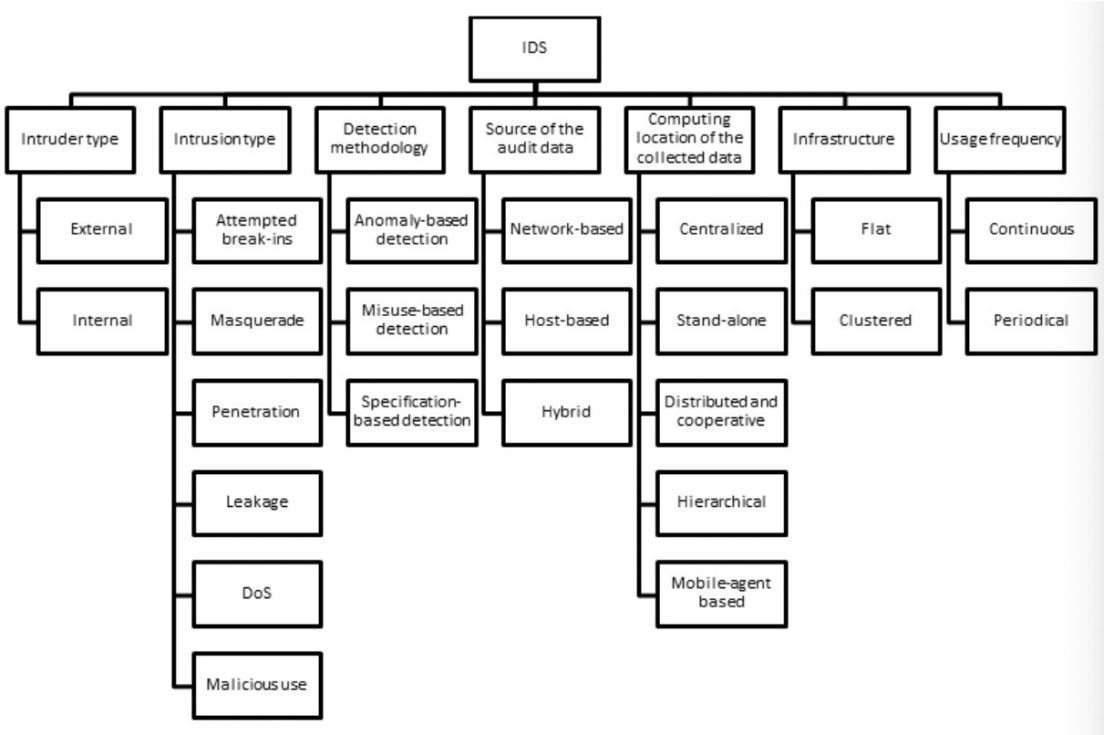

Figure 5. IDS taxonomy for WSN [136].

Intruders are divided in internal and external, depending on the access they have to the network: externals need to use different means of attacks to reach the network. Intrusion type indicates the way an intrusion can happen in a network. IDS may provide partial detection solution,

according to intrusion type. Anomaly-based detection, misuse-based detection, specification-based detection are the three parameters of detection methodologies, or else, statistical behaviour modelling, signature-based (of the previous known attacks) and a set of specification and constraints, accordingly. Depending on the location of the data to be analyzed, IDS categorizes in three group the sources: network, host or hybrid, which are considered as the three categories of source of the data. Computing location of the collected data: five categories of IDS according to the computing location of the collected data, centralized IDS, stand-alone IDS, distributed and cooperative IDS, hierarchical and mobile-agent based. The infrastructure could be flat or clustered [160], depending on nodes, considered as equal or not. Usage frequency could be continuous or periodical. IDS need this information in order to monitor either 24/7 or in certain periods of time.

The taxonomy in [129] uses datasets in order to identify threats and tools underrepresented in currently available research, help researchers building IDSs and associating the threats to the OSI model. Training against real-world threats was also one of the goals of the taxonomy, however only 1/3 of known attacks are covered and zero-day attacks can't keep up in this taxonomy. The key thing is that the authors focus on the source of the attack, dividing the threats into network, host, software, physical and human ones.

Network threats: Threats are initiated based on a flow of packets sent over a network. Two of the most common forms of network threats are Denial of Service (DoS) and Distributed Denial of Service (DDoS). Host threats: Host attacks target specific hosts or systems by running malicious software to compromise or corrupt system functionalities. Malware is the most common host attack. Software threats: Code injection can include SQL Injection to query or to a whole database, which would lead in obtaining confidential data, or deleting data by dropping columns, rows or tables. Cross-site scripting (XSS) is used to run malicious code to steal cookies or credentials. Physical threats: Physical attacks are a result of a tempering attempt on the network hardware (edge, or other devices) or its configuration. Human threats: The last category of networking attacks is based on human actions. These include user masquerade or phishing.

The taxonomy in [131] is an update of an older taxonomy, trying to keep IDS up due to fast-paced changing environment, so the IoT domain is now part of this IDS classification. Its basic differentiation is that the authors have expanded the IDS taxonomy by adding the target system, which now considers the IoT domain. This taxonomy matches with the one in [136], as they both use detection methodology in their classification, intruder type/deployment approach as well.

Kjaerland in [173] suggested one type of taxonomy from the Computer Emergency Response Team (CERT) for cyber breaches. This kind of technology relies more on user profile to identify

victims and fraudsters. Attacks were employed inside this taxonomy using the operation, target, source, and impact methods together with aspect theory and multidimensional scaling (MDS). This means that it evaluates the degree to which specific examples are comparable to one another [174] and the methodical approach to harmonizing theory and research [175]. Each feature has a certain number of components, each with a detailed explanation. These characteristics were used by the developer to contrast the government side with the business side. In order to determine why, how, and where attacks occur, Kjaerland's technique focuses more on user behavior and determines what their aims are [176]. This method, like others, has disadvantages, including a high-level perspective of the taxonomy of operations that omits a detailed explanation of the techniques that can be used to identify the attack's basis.

Another taxonomy was presented, using four distinct dimensions that, when combined, provide an all-inclusive category by encompassing network and computer attacks developed by Hansman and Hunt [177]. Their particular taxonomy aids in enhancing computer and network security and uses ordinary language with an attack justification. The first component of the method that is used to group an attack is called an attack vector, and the second component of the approach groups the target. The vulnerability classification number is listed in the third dimension, and the attack's effects are highlighted in the final dimension. A drawback of their methodology is that each level of the taxonomy contains a thorough explanation of the attack [178]. The method's last drawback is that not enough information is provided, making it unable to gather data for defense against attacks.

A taxonomy for DDoS attacks, as well as the defense tools used to categorize the attacks and the many defense tactics involved, was proposed by Mirkovic and Reihner [179]. This particular approach provides a summary of the characteristics and attack tactics that are employed inside the method. As a defense mechanism, strategies are crucial. In order to categorize DDoS attacks, this method makes use of a degree of automation, exploited holes, source address validity, attack rate dynamics, the possibility of characterization, persistent agent set, victim type, and impact on the victim. The developers also developed a defense that offers deployment location, collaboration level, and activity level. The grouping employed in this approach, which is used to aggregate DDoS attacks and defense within a method, offers a way for researchers to communicate and debate solutions.

Validation Exposure Random Deallocation Improper Conditions Taxonomy, more narrowly known as VERDICT [180], which was developed by Daniel Lough, can be used to classify attacks. This strategy concentrates on four areas that are displayed as security flaws. These include incorrect deallocation, incorrect exposure, incorrect randomization, and incorrect validation. These four categories stand out easily because they are labeled "improper," which indicates that the attacks take place in an inappropriate setting. Physical security is included in

the taxonomy of attacks, however validating attacks within it might be done erroneously or with biased data [181]. The second component of the taxonomy, incorrect exposure, can be utilized to disclose an attack directly or indirectly depending on its vulnerability. The cryptography of the attack and the inconsistent use of randomness involved are covered in the third section, which is called randomness. The last section is titled improper deallocations, which refers to incorrect data demolition or residuals, which also includes trash diving. The vulnerability in the method can be explained in a number of different ways according to this taxonomy. This method's lack of a classification of attack kinds, including Trojans, viruses, and other threats, may be a drawback.

2.4.3 Cyberattacks/CTI Taxonomies

In [147] the main theme of the taxonomy is cyberattacking. The authors are based on the access level of the attacker and they propose a 3-tier taxonomy, from *no access* to *user access* to *root access*. The taxonomy was initially created to help military network defenders organize their defence strategies against a variety of threats. The taxonomy also gives the military modelling and simulation community a framework, on which they can base their approaches when asked to model the impacts of a specific cyberattack. Due to the magnitude of these attacks, this taxonomy's drawback is that it only concentrates on well-known attacks and gives rudimentary information.

In the first tier, no network/computer access is required for the attacker and the attacks included are DoS, DDoS, Stack-Based Buffer Overflow Attack and Phishing. The second tier includes the following attacks, requiring user access with limited privileges: password hacking, sniffing and nuisance attacks. The root access/administrative privileges tier includes backdoor, rootkit, kernel-level rootkit, spyware and keyloggers, adware, various malicious attacks, delivery methods, trojan horses, viruses, worms and scareware.

[149] classifies known attacks and their attack subcategory. This taxonomy was created for network administrators, software developers and users, to help detect and avoid future cyberattacks. After analyzing the performance of malicious cyberattacks, they have produced a sophisticated taxonomy, including: information foot printing and reconnaissance attacks, information scanning attacks, enumeration attacks, information system attacks, trojan and backdoor attacks, virus attacks, worm attacks, sniffer attacks, social engineering attacks, denial of service attacks, session hijacking, webserver vulnerabilities, web-based applications attacks, intrusion detection systems-firewalls and honeypots attacks, buffer overflow attacks and physical attacks. All those categories in the next level are analyzed as of their attacks subtype. There is one thing in common with [147], the taxonomy is talking about basic cybersecurity attacks and known vulnerabilities.

[143] proposes a novel taxonomy approach to Mobile Ad hoc Networks (MANET) attacks, called Attributes-Based Taxonomy. This taxonomy represents each attack as a vector that consists of six classification attributes, namely, the legitimacy of attacking node/s, the number of nodes participating in the attack, the MANET vulnerabilities utilized by the attack, the network resources exploited by the attacking node/s, the targeted victim and the network security service compromised by the attack. The major drawback of this approach is that it is possible that some attacks do not generate any anomalous basic events. They classify based on the attributes an attack has, so here are the 6 categories of attributes the authors have found and made this taxonomy: legitimacy of attacking node/s, number of attacking nodes, exploited MANET vulnerabilities (EMV), exploited network resources (ENR), targeted victim (TV) and compromised security service (CSS). The differentiation of this taxonomy is that no other known taxonomy focuses on the effect an attack has on a victim or the network.

The taxonomy in [151] hopes to aid data mining processes in cybersecurity and big data projects. There are 7 classifications that wrap up the incident, 6 that wrap up the attack and 2 that wrap up the event. They use hierarchical clustering as a method of classification and the differentiation of this taxonomy is the different motivations of attackers included. The classification starts with the event, which includes the action and the target. Event is part of attacks, which also consider tool, vulnerability and unauthorized result. Then we have incident, which includes attack, event, plus attackers and objectives. Overall, this taxonomy states that different motivations of hackers, source characteristics and target country characteristics lead to different likelihoods of attacks on different organizations. Timely reporting of cyberattacks to authorities is thus likely to strengthen the rules of law and help combat cyber threats in the long run.

The Detection Maturity Level (DML) model (Figure 6), which highlights the rising level of abstraction in the detection of cyberattacks, was expanded by the authors of [132]. In this expansion they introduce the new highest level of this taxonomy, DML-9, which stands for the attacker's identity. The important point is that, in terms of low-level technical observations, the abilities required to detect a cyberattack decrease with decreasing levels of abstraction. The lack of connections between motives, objectives, and attack techniques in this taxonomy is a flaw. The objective of this taxonomy, which is to assist risk management in identifying threat agents pertinent to particular assets, would not be hindered by this, though.

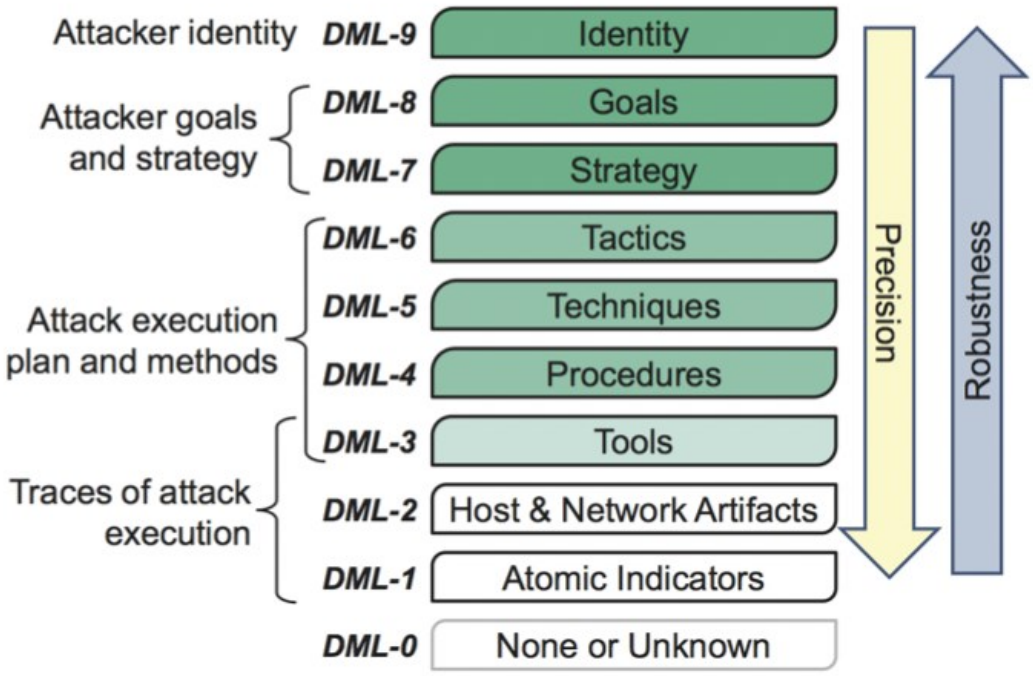

Figure 6. DML model updated [132].

A collection of uniform definitions and descriptions for important threat agents is called the Threat Agent Library (TAL) [161]. The collection is not intended for identifying persons or looking into actual security incidents because it does not reflect specific threat actors. TAL's objective is to assist with risk management, specifically by identifying threat agents pertinent to certain assets. Security experts can proactively create protections against particular threats in this way. TAL library's "hostile" threat actor categories can be utilized in conjunction with Mitre's ATT&CK taxonomy, which compiles a list of recognized threat actors and their recognized strategies. A new taxonomy that categorizes threat actors would be introduced as a result of the linkage of the two aforementioned taxonomies.

A brand-new taxonomy for cyberthreat motivations was presented by Casey in 2015 [162]. The taxonomy outlines the motivators that lead threat actors to engage in unlawful behaviour. Understanding these drivers may help to identify the type of harmful actions to be anticipated.

Common IDs for widely publicized information-security vulnerabilities in software packages are provided by Mitre's Common Vulnerabilities and Exposures (CVE) dictionary [163].

Databases of security checklists, security-related software defects, misconfigurations, product names, and impact measurements (CVSS) are all part of NIST's National Vulnerability Database repository (NVD) [164]. NVD is built upon CVE and integrates CPE, as well as CWE into the scoring (impact metrics) of CVE entries.

For naming and encoding IT product classes, Mitre's Common Platform Enumeration (CPE) [165] specification defines standardized machine-readable techniques (software and hardware).

In order to better comprehend software defects and provide appropriate countermeasures, Mitre's Common Weakness Enumeration (CWE) [166] is a dictionary of software security weaknesses and vulnerabilities. Their dictionary includes descriptions of the attacks, the conditions that must be met to carry them out, and mitigating techniques.

The most prevalent methods (techniques) utilized in cyberattacks deriving from CWE are included in Mitre's Common Attack Patterns Enumerations and Characteristics (CAPEC) [167]. Similar to CWE, CAPEC provides summaries, prerequisites for attacks, and remedies (countermeasures) for the most typical attack patterns.

Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) by Mitre [168] offers a list of recognized actors, their known tactics (10 tactic categories), and post-compromise methods to accomplish their goals. The distinction between CAPEC and ATT&CK is that the first offers thorough coverage across a variety of post-compromise approaches while the latter enumerates a variety of attack patterns over the complete cyberattack life cycle. The tools utilized by distinct threat actors and linked to certain approaches are included in addition to the techniques seen in ATT&CK. The correlation between detected indicators and TTPs and threat actor identities is made possible by these taxonomic relationships.

A 3-dimension taxonomy is described in [141], which is based in traditional triangle of confidentiality, integrity and availability. The authors have added two additional dimensions in each, to offer a more complete view of data security. The scope of this taxonomy is to provide a comprehensive basis for cyberattacks and have better security measures. The biggest asset of this taxonomy is that it can be applied to any attack or any system.

This taxonomy is based in Cyber Defence Capability model [169], which is a study of Kolini & Janczewski and it is a taxonomy of security measures. Their study expanded upon the United States Airforce Cyber-Kinetic Reference Model. Their model included the following major areas: assets, capabilities, and actors. From these three categories (Assets, Capabilities, and Preparation Process) there are subcategories.

This taxonomy focuses on security measures rather than attacks. It starts with defining assets, which the authors classify into four groups: people, information, software, and hardware. The capabilities that can defend those assets are connected to the assets category. The taxonomy they provide covers the most ground here. The four main categories of capability are actors, passive defence, active defence, collaborative defence, and active defence. Each of those is further broken down. The preparation process is the last significant category in the taxonomy suggested by Kolini & Janczewski. This explains how to put security controls in place. A taxonomy for examining and comprehending security controls is offered by Kolini and Janczewsky. The McCumber cube was mentioned in their study, although it was not the main model used.

Papp, Ma, and Buttyan created a taxonomy specifically for embedded systems [170]. They investigated assaults on embedded systems based on their responses to four questions. The following topics were looked into: What are the main causes of successful attacks, what are the main vulnerabilities, what are the traits that these attacks share, and how can this information be used to improve embedded system security.

Papp, Ma, and Buttyan began their taxonomy by searching the CVE database for vulnerabilities that have been disclosed in embedded systems. They found 3.826 of these vulnerabilities. The following criteria were used to categorize attacks: precondition, vulnerability, target, attack method, and attack effect. Any prerequisites that must be met in order for the attack to be carried out are included in the precondition dimension.

The AVOIDIT taxonomy was developed by Simmons, Ellis, Shiva, Dasgupta, and Wu [171] and examined five parts of an attack: Attack Vector, Operational Impact, Defense, Information, Impact, and Target. An overview of the attack's components is provided by the six-dimension taxonomy, which is an advance on the prior taxonomy. According to Simmons et al., any suggested taxonomy had to possess the property of mutual exclusivity in order to be a successful taxonomy. The writers intended this to imply that an attack could only fall under one category.

The ADMIT taxonomy was proposed by Joshi & Singh [172]. Attack vector, defense, technique, impact, and target were the five dimensions of the taxonomy.

2.4.4 IoMT Taxonomies

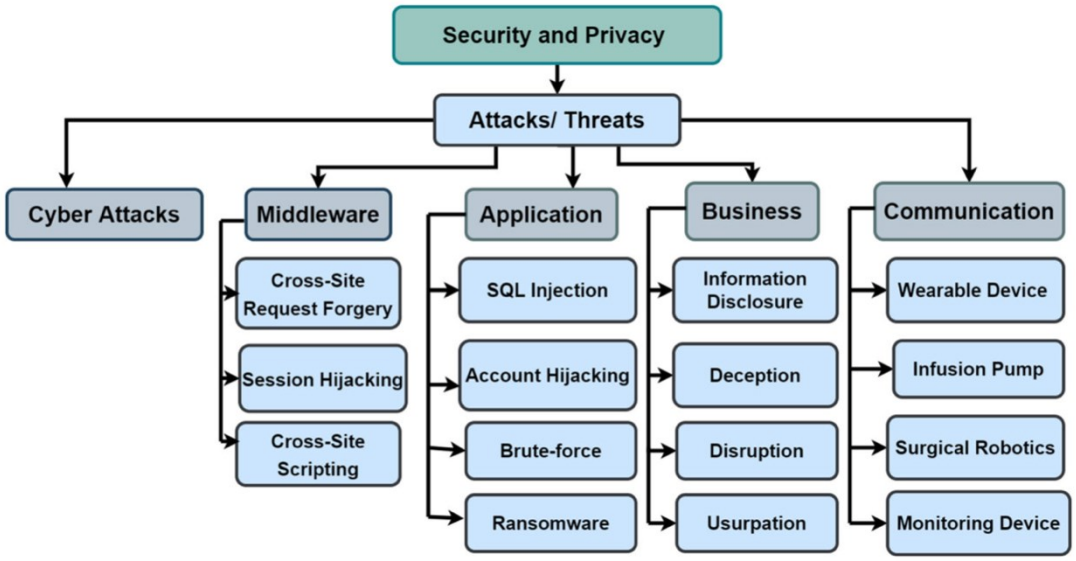

Figure 7. Taxonomy of IoMT Security and Privacy [12].

In [12] the authors describe a taxonomy of IoMT security and privacy (Figure 7) which divides attacks and threats in 5 categories: cyberattacks, middleware, application, business and

communication. Middleware level collects and filters data from sensors (perception layer), discovers services, and controls device access. Application layer is the user-friendly interface for IoMT devices, connecting people through a middleware layer, so the taxonomy classifies 4 well-known attacks in this level, SQL injection, account hijacking, brute-force attack and ransomware. Then we have business layer, which handles the business logic of the healthcare provider and enables the lifecycle of the business process, including monitoring, management, and improvement. It is also responsible for gleaning insights from IoMT data. Attacks on this layer have been investigated in the past, but because they involve sensitive medical data, their impact is greater. Possible attacks include information disclosure, deception, disruption, and usurpation. In communication layer is included every harmful action that tries to get access to a medical device using communication layer protocols in order to disable it, steal medical data from it, or otherwise damage it. All the other attacks, known or not, are included in cyberattacks.

Overall, this taxonomy includes basic information about an attack/threat and categorizes it upon the layer, but it is generic and lacks extra information about the intruder (motives etc.). However, the goal is a representation of security and privacy issues of IoMT, which can be expanded in the future.

[13] presents a taxonomy of security threats in IoMT edge network (Figure 8). Cybersecurity represents confidentiality, integrity, authentication, authorization and availability in [13], so the taxonomy classifies each known attack according to the security objective that the attack intends to compromise. The goal of this taxonomy is to enable countermeasures against those threats to IoMT networks. The drawback of this taxonomy is that there are some attacks that could be categorized in two or more levels, as sometimes they compromise more than one security objective. However, the representation itself is clear and the taxonomy can be easily expanded in the future if new attacks come up.

[20] suggests a taxonomy to categorize the cybersecurity attacks in IoMT. The first level of this taxonomy includes nature of the attack, target, scope, impact and capacity of the attacker. The goal of this taxonomy is to categorize each attack and mitigate it. It is a very generic taxonomy and can be easily expanded.

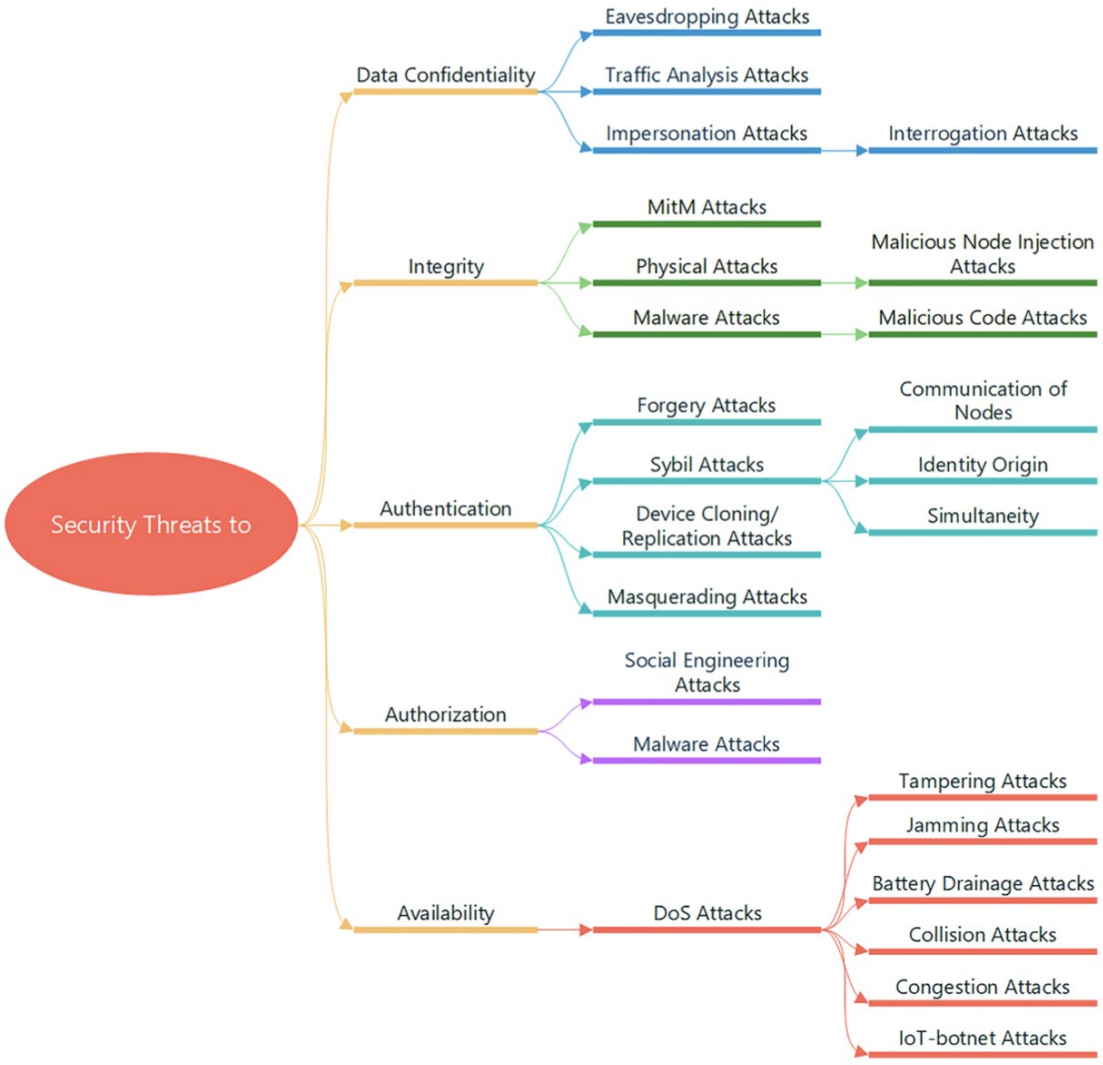

Figure 8. Taxonomy of security threats in IoMT edge network [13].

Authors of [26] suggest an interesting taxonomy for security and privacy in IoMT with 9 categories in the first level (Figure 9). It is the only taxonomy in IoMT and cybersecurity domain which includes both security and privacy separately. They have divided the information that can be gathered from this taxonomy in: IoT layer, intruder type, compromise level, impact, attack method, CIA compromise, attack origin, attack level and attack difficulty. It is a completed taxonomy in first depth but also it is tested in real-world incidents, which is a huge plus, as it was first designed for risk assessment scope. It is an updateable taxonomy and can be expanded to comprehend new attacks, devices and services as well. The authors also note that they have presented this architecture as of layers, as each layer provides specific functionality which has distinct security and privacy issues.

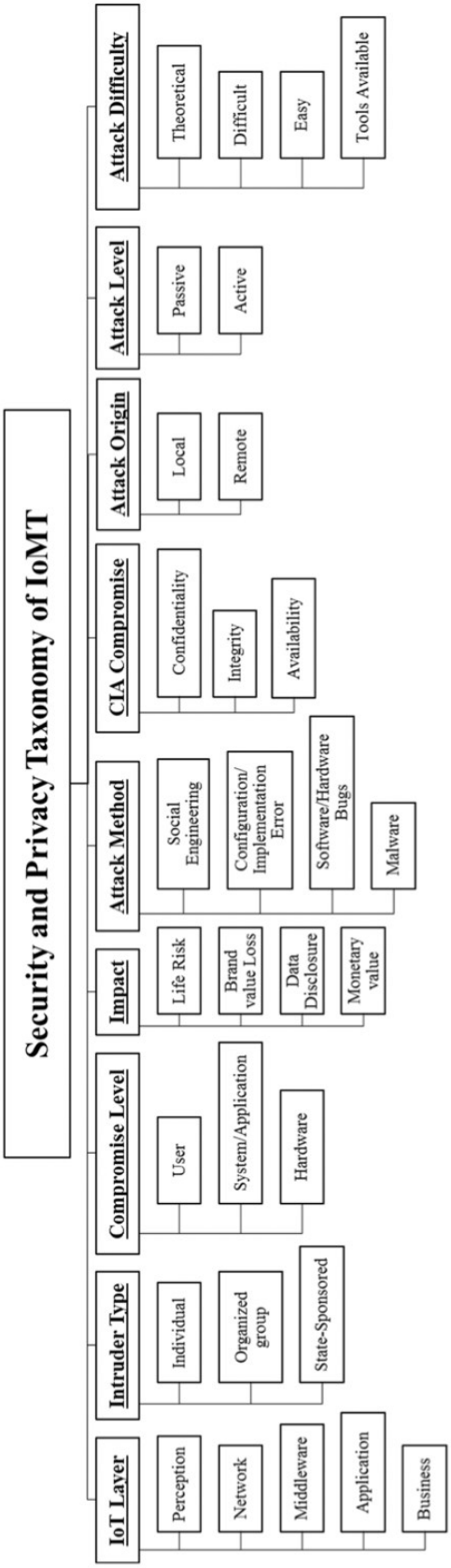

Figure 9. Security and privacy in IoMT taxonomy [26].

3

IoMT Cybersecurity Taxonomy

IoMT is a new paradigm in technology, where only a few security research has been done on it, while device manufacturers have rushed to create IoMT solutions without thinking about security. Since sensitive and private data is constantly transmitted inside the IoMT ecosystem, it is a top target for attackers [22].

Running encryption algorithms is one example of a security calculation that makes use of a large percentage of the computational resources. Because many of these IoMT devices have constrained computational capabilities (low CPU power, memory, etc.), execution cannot be completed in those resource-constrained settings. Weak encryption methods are utilized widely, leaving devices open to malicious assaults [22].

We have created a taxonomy which includes 9 categories in the first level (Figure 10): attack nature, attack type, attacker's motivation, communication, attack method/target layer, compromise level, impact, damage range and countermeasures. The differentiation compared to other IoMT cybersecurity taxonomies is that it can work serially (after you detect the first category, then move to the next etc., until you have the right countermeasure for mitigation), but this is not absolute, its categories can also help autonomously to identify an attack. In addition, our taxonomy covers the attack itself, attacker's motivation, communication protocols of the devices, the end user (as of compromise level, impact and damage range), the company that produced the device (as of compromise level, impact and damage range). This spherical thinking is unique for taxonomies, as mitigators usually focus on the attack or the attacker or the device.

First thing to identify is the nature of the attack, so we can understand where there are vulnerabilities in the network and anticipate the next levels or some of them. For example, if an attack is external and it is passive, it is possible that the network layer is compromised and the attacker is trying to eavesdrop. This information, combined to the attacker's type and

motivation we can anticipate the compromise level, the impact and so the damage range. All those information can help us mitigate with the right countermeasures.

A difficult category to anticipate though is communication protocols compromised, which is inextricably linked to the IoMT device capabilities, type and sensors. It is common for the most IoMT devices to use cloud to store the patients' data and share with doctors/nurses/hospitals, so apart from the first level of communication between the IoMT device and the user (for example a BPM which is connected to a smartphone via Bluetooth and shares real-time blood-pressure values), there are some data stored in the cloud, for the doctor to access history of blood-pressure values for the past two months, in case of emergency. So, cloud, with all its vulnerabilities is essential for IoMT and because it stores big amounts of data, it can be an easy target for an attacker.

The taxonomy we have created helps in both proactively preparing for security in IoMT, identifying the motives and objectives of attacks and mitigate them. This classification can also assist to prepare the system and use countermeasures for similar attacks in the future.

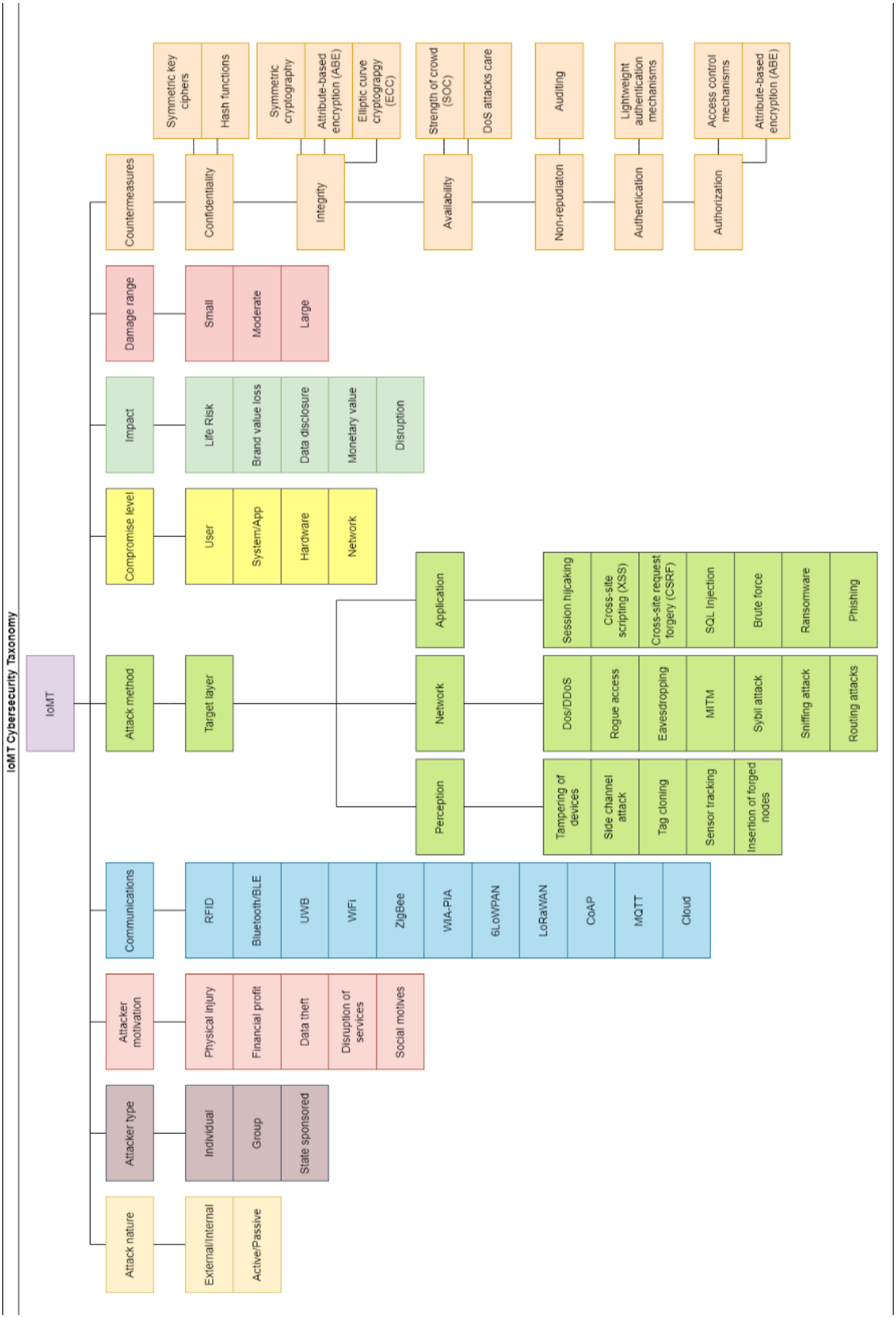

Figure 10. IoMT Cybersecurity Taxonomy.

3.1 Attack nature

Attackers are divided into two categories based on their point of attack, their motives and goals as well [26]: internal or external and passive or active. In some cases, many attacker types may cooperate together to assure a more complex cyberattack [21].

3.1.1 External/Internal

External attacks are described as harmful intrusions that use worms, rootkits, or Trojan-attacks to gain access to a hospital system, violate sensitive patient data, and spread or sell it to a third party with an ulterior goal for use in frauds [20]. There are also cases where the attack makes use of phishing techniques by submitting fake PDFs or CVs. A key recorder or back door can be placed on the desired machine after the download is finished. The attacker does not require physical access to the medical device or administrator privileges to the system. Instead, he will attempt to remotely attack any system flaws or weaknesses [29] using malware or vulnerabilities to remotely exploit system flaws [26].

For an internal attack to succeed, the attacker must be nearby or nearby to the target device and have some authority to access the network infrastructure. It might be a genuine user, like a nurse who improperly accesses the medical records of a famous patient [29] or member of the medical staff, who aims to harm a hospital's reputation by erasing or altering data or by targeting the health and privacy of patients [21]. When an attacker is close to medical equipment, they have the option of causing physical harm or gathering data to conduct subsequent distant attacks [29] or gather data about the area to be utilized in a remote attack [26]. In rare instances, a spy disguising themselves as a nurse or doctor, thwarting all hospital security procedures to eliminate a specific patient for either political or other criminal motives. Internal hackers could make it easier for external hackers to carry out cyberattacks [21]. So, to easily carry out their cyberattacks, internal attackers might easily be exterior attackers as well or collaborate with them [20].

3.1.2 Active/Passive

The active attacker poses a greater threat because he depends on intercepting patient data and later altering, erasing, or changing it. This can be exceedingly risky and occasionally even fatal. The hacker will intercept network signals and instruct the wearable device, change messages sent before they arrive at the remote system, or stop messages from going in the direction they were supposed to go. A successful intruder has a variety of goals [29]: for instance, it may result in the wrong drug being supplied to a patient or the administration of a greater amount of medication, endangering the patient's life and possibly even resulting in death [20]. In addition,

he may indiscriminately ask the medical equipment for information to drain its power [29]. Attacks that are currently active include DDoS, brute force, buffer overflow, and SQL injection [26].

A passive attacker works to avoid detection by remaining still and "hidden" in the background. The goal is to read and build up their own information gathering process from data that is being communicated between various medical devices via any wireless connectivity, then intercept it with the possibility of developing into a far more complex cyberattack. As part of the information gathering process, passive attackers may collaborate with external or even internal attackers [20]. Passive attackers' main goal is to gain access to another system component or to gather intelligence for launching active attacks on the system or pose a privacy threat [26]. Examples of passive assaults include man-in-the-middle attacks, sniffing, packet interception, and snooping. It would be realistic to say that a passive attacker can immediately compromise communication confidentiality by merely viewing the content of messages. He will have access to private data including the medical device's model and serial number as well as the ability to record telemetry data. He can also record the patient's personal information, including name, age, and medical history. The end effect in each of these situations is a serious breach of the patient's privacy [29].

3.2 Attacker type

3.2.1 Individual

A single perpetrator of an assault. Individuals have the least capabilities, compared to other 2 categories. Blackhat hackers or spies rely on this category.

3.2.2 Group

An organized group is a collection of people who have come together to launch an attack and are typically more powerful as a whole. A good example of organized groups are hacktivists.

3.2.3 State sponsored

Individuals who are sponsored or linked with the state frequently have goals that coincide with economic or political agendas. This kind of intrusion is extensively sponsored and equipped to conduct significant attacks like DDoS.

3.3 Attacker motivation

3.3.1 Physical injury

It is possible for medical equipment to be hacked and used against someone. Patients may be threatened by nefarious parties that have political, criminal, or, in certain circumstances, terrorist motivations. These assaults can be useful instruments for a variety of illegal activities, such extortion or coercion [29].

3.3.2 Financial profit

Attackers or competitors of Implementable Medical Device (IMD) vendors are heavily influenced by economic and financial gain when making such threats. If an attacker has access to medical information, they might use it to blackmail the patient or sell the information [29].

3.3.3 Data theft

Medical equipment uses a variety of criteria to gather important data about a patient's body. The patient's diagnosis, management, and/or operational or surgical procedures may require this information. Medical records include details about a patient's behavior. For instance, a pacemaker's data analysis will show the patient's past history of physical activity. If collected in a sufficient sample size across many device kinds and marks, such data can be utilized to identify both general and specific patterns in the well- being of individuals and groups. Sensitive data may be used in unlawful and unethical ways as a result of this kind of information [29]. Also, wireless transmissions of messages from medical equipment are transmitted to the system controller. Normally, these interactions give patients' positions and health information, so if these communications are intercepted by attackers, a patient (or more) can be tracked live.

3.3.4 Disruption of services

When an IoMT device stops its service, the patient(s) is facing a (D)DoS attack, which is preventing them from receiving the right medication. This could lead to a life-risk situation. At the same time, the doctors or the nurses would be unable to access the medical records and prescribe another treatment.

3.3.5 Social motives

Attackers intention sometimes are strengthened from social motives. Some examples of these motives are political religions and hacktivism.

3.4 Communications

3.4.1 RFID

Using radio frequency signals for very close- range communications, Radio Frequency Identification (RFID) is a wireless object identification method [33]. The development of body health systems depends heavily on autonomous RFID tag technology that is positioned inside or close to the patient's body [34]. Additionally, passive RFID tags can be employed for a variety of applications, including patient environment monitoring, physical access management, and monitoring the storage temperature for various drug types [35, 36]. The usage of RFID technology makes it challenging to integrate typical security measures in devices with very low power features. Researchers have, nevertheless, put forth a number of significant bespoke authentication schemes. [37] makes a proposal for an RFID tag authentication technique that requires less memory and processing on the tag side. This protocol offers privacy and security features in addition to defenses against replay, DoS, forward and backward tracing, and server impersonation. On the other side, [38] presents a hash-based RFID security mechanism with forward privacy. Its primary objective is to defend the RF tag against tracking assaults by keeping records of prior unsuccessful tag sessions. Furthermore, [96] identifies and suggests partial solutions to several restrictions. Dynamic passwords, synced secrets, and unique system authentication mechanisms are a few examples.

3.4.2 Bluetooth/BLE

Bluetooth is a wireless communication technique based on the IEEE 802.15.1 standard. Low power and cheap cost are among Bluetooth's characteristics that can send data between mobile devices over a close range (8–10 m with 2.4 GHz band). The most affordable and low- power variant of this standard (also known as Bluetooth Smart or BLE) is Bluetooth Low Energy [39]. The IoMT devices like Internet of Wearable Devices (IoWDs) and human interface (HID) devices are also better suited to Bluetooth/BLE thanks to these features [40]. BLE is vulnerable to attacks and may endanger the connected devices. These vulnerabilities cut across all communication layers as well. However, BLE implementation offers a number of security safeguards to reduce such threats [41]. Some methods use AES-CCM encryption to achieve confidentiality and integrity. Furthermore, the authors in [42] offer a selection of methods and defenses that can be applied to secure Bluetooth connections in order to defend Bluetooth Low Energy (BLE) technology from attacks.

3.4.3 Ultra-wideband

The IEEE 802.15.3 standard, which has lately gained favor as a form of high-speed, short-distance indoor wireless communication, is the foundation for UWB (Ultra-wideband) technology [43]. One of the most exciting features of UWB is its bandwidth, which is more than 110 Mbps and suitable for hospitals and most multimedia recommended for medical systems in [44] because interacting with implanted sensors requires a methodology that goes beyond channel restrictions due to severe signal attenuation. A microcontroller receives signals from sensors, which is how it operates [36]. UWB faces threats from attacks that take into account the distances between nodes because it is a distance protocol. UWB utilizes the block cipher for the Advanced Encryption Standard (AES) with counter mode (CTR) and cipher block chaining message authentication code (CBC-MAC) [45]. A Verifiable Multilateration (VM) technique is proposed in [46] to identify a distance augmentation attack using verification triangles. Other publications like [47, 48] suggest a location-based secure authentication technique to thwart outside attacks. Additionally, [49] advocates using pulse reordering as the first modulation strategy to prevent ED/LC (Early Detect/Late Commit) assaults in the UWB, independent of communication range (UWB-PR).

3.4.4 Wi-Fi

Based on the IEEE 802.11 family of standards, Wireless Fidelity (Wi-Fi) is a middle-range (up to 100 m) protocol [50, 51]. Wi-Fi has been suggested by a number of authors as a means of connecting monitoring equipment in an IoMT system. For instance, the authors in [52] demonstrate the effectiveness and security of this protocol by using it on a network of 45 crucial medical care equipment. Additionally, this protocol is used in connection with the Global System for Mobile communication (GSM) in a system for remote patient health monitoring to simulate the transfer of medical data between two separate geographic locations [53]. The technologies used to safeguard Wi-Fi 802.11 communications include Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3). More potent encryption techniques are a feature of WPA technology [54].

3.4.5 ZigBee

The IEEE 802.15.4-compliant ZigBee wireless communication protocol is designed for low-power, low-cost, and low-speed wireless personal area networks that connect devices primarily for personal usage [55]. Health zones employ this protocol to link sensors to the coordinator and also among the coordinators [56]. The ZigBee Health Care Profile, which implements a fully functional application layer protocol for healthcare environments, is built on ZigBee Pro [57]. ZigBee employs the IEEE 802.15.4 standard to implement higher layers in order to

guarantee MAC layer security. When security methods are applied, symmetric key cryptography is performed using AES. The authors of [58] provide a framework that can anticipate and guarding against a variety of potential harmful assaults in the ZigBee network, as well as reacting properly by alerting the system administrator. Additionally, based on real-time data specified by the system administrator, it is capable of making instantaneous automatic judgments.

3.4.6 WIA-PIA

An industrial wireless communication standard for process automation developed in China is called WIA-PA [59]. The work in [60] suggests WIA-PA as a transmission protocol in the internal networks of wireless sensor networks, in medical remote monitoring system, despite the fact that it is an industrial protocol. The MAC layer security of the WIA-PA network is based on IEEE STD 802.15.4-2006. It offers two tiers of security services above the MAC layer: point-to-point security in the data connection sub layer and end-to-end security in the application sub layer (DLSL). Additionally, WIA-PA offers the entire network a secure access authentication system [61]. For device authentication, Wang et al. developed the WIA-PA architecture [62]. Utilizing a join key that is shared between a device and a security manager, access is granted through WIA-PA.

3.4.7 6LoWPAN

6LoWPAN is an IPv6 adaption layer that specifies ways to enable IP connectivity for devices with limited resources when they are using low-power, lossy channels like IEEE 802.15.4 [36]. IoMT sensors and local devices can be connected to IP networks in the healthcare industry using 6LoWPAN [63]. Furthermore, 6LowPAN permits the connectivity of sensors with middleware devices or routers that are linked to the Internet [64]. The 6LoWPAN stack's various tiers have security procedures built for it. While the upper layer security is intended to provide end-to-end security between two remote peers, the MAC security sub layer of IEEE 802.15.4 is defined to provide hop-to-hop security for the wireless channel [65].

3.4.8 LoRaWAN

Originally created by Semtech, LoRa (Long Range) is a physical layer protocol meant to support low- power and broad area networks. Contrarily, LoRaWAN specifies both the system architecture and the network's communication protocol [66]. [67] presents a loT-based health monitoring system. In this system, the secure, inexpensive, and low-power communication channels provided by an established LoRaWAN network are used to transmit the medical data gathered by sensors to an analysis module. For complete network security, including mutual

end-point authentication, data origin authentication, replay and integrity protection, and privacy, LoRaWAN leverages the 128-bit Advanced Encryption Standard (AES128). Each LoRaWAN device is uniquely identified by a 128-bit AES key (referred to as the AppKey) and a globally unique identification based on EUI-64 [68].

3.4.9 CoAP

In the IoT with fewer nodes and networks, the Constrained Application Protocol (CoAP) protocol was initially developed for web transport. The need for a lightweight, low-rate protocol as well as the strict criteria of the IoT were the initial driving forces for the creation of this protocol. The IoMT restricted nodes with less memory and processing power are specifically suited for this protocol [69]. In a system that is suggested in [70] for safeguarding real-time health monitoring systems, CoAP and the MQTT protocol are utilized to safeguard sensor data from security breaches throughout its continual transmission over the layers. Strong authentication methods should be used to prevent breaches like data theft and DoS attacks. To find any malicious activity in the system, it is advised to utilize an intrusion detection system [71].

3.4.10 MQTT

A publish/subscribe Push protocol known as Message Queue Telemetry Transport (MQTT) was created by IBM in 1999. MQTT was created to convey data accurately even with extended network delays and constrained capacity, therefore IoMT developers employ it because of its low memory use and low bandwidth requirements [69]. The work given in [72] creates a medical application built on the Blockchain that uses MQTT to link a variety of devices to an IoMT platform. A method to connect a remote healthcare unit as if it were located inside the hospital was also proposed in [53]. This system employs the MQTT protocol to send measured data from the healthcare unit to the hospital's gateway. Unfortunately, the MQTT protocol does not by default encrypt data in transit and only enables authentication for the security method. Implementing this protocol presents questions about data integrity, secrecy, and authentication. The TLS/SSL protocol is used by MQTT brokers to perform authentication using username and password [73].

3.4.11 Cloud

The authors of [74] highlight the issues contemporary healthcare systems confront as a result of the vast amount of unstructured, varied, and exponentially rising data. Medical professionals are unable to keep up with the continual influx of data from sensors. Understanding the vast amount of produced unstructured data is quite difficult. As a result, it becomes essential to use

a variety of data storage technologies for effective memory allocation and data management. The cutting-edge methods and large capabilities of cloud computing are used to solve this issue. Large amounts of data can be processed more quickly to facilitate Big Data analytics by using cloud technologies. [74] makes the case that improved feasibility and data security may be attained if data is kept in a single, central location as opposed to being disseminated. Since it is crucial to maintain the confidentiality of patients' sensitive medical information, cloud platform encryption features are highly sought after. Additionally, a cloud architecture would incorporate efficient use of the cloud's storage space by reducing data redundancy. This development creates a single, centralized database, opening the door for the integration of AI into healthcare systems. In such an AI-enabled environment, the intelligent monitoring systems offer the patient predictions and diagnoses based on the traits deduced from the sensor data. Without a cloud platform, an IoT architecture is analogous to a car without petrol. In actuality, it is the data collected by IoT devices and kept in the cloud that is helpful in extrapolating significant information from the data and doing trend analyses on the data. Where cloud computing services excel is in data analytics. By handling complex tasks that call for storing, processing, and analyzing the system-collected patient health data, the cloud frees up the IoT subsystem from demanding computing [75]. The processing and analysis of the data acquired by IoT devices are thus made possible by cloud platforms, which offer the computational infrastructure, database, storage, and applications required. In simple terms, a cloud is a network of strong servers that is connected and provides a variety of necessary services. The following three primary services are [76]:

- Infrastructure as a Service (IaaS): Charged with giving the cloud access to real infrastructure like servers, storage, etc.
- Platform as a Service (PaaS): Provides certain tools and functions to the cloud-based infrastructure, including virtualization, networking, database administration, etc.
- Software as a Service (SaaS): Allows web-based programs to access the gathered data and carry out various operations on it.

  The cloud architecture used in healthcare systems typically includes the services described above. It is crucial to permit authorized users to work with and manipulate the health data produced by a few sensors for an IoT-based patient monitoring system. SaaS excels in this area by offering web-based applications to access and work with that data. Similar to this, PaaS is used to manage these enormous amounts of data because it contains the capabilities required for this operation, including virtualization and database administration. The importance of IaaS may be deduced from the aforementioned application since it offers a physical infrastructure, such as servers and storage for the data, and is the fundamental building element of any cloud-based system. In an IoT environment, these numerous services

can be used to complete a variety of activities. However, big data management and data processing are the two main uses of these services in health management systems [52].

3.5 Attack method/Target layer

3.5.1 Perception

The perception layer oversees gathering critical body parameters from the patients utilizing physical IoMT devices, such as body temperature, blood pressure range, blood oxygen level, heart rate, and blood glucose level, etc. The network layer receives the accumulated data and transmits it to the final location [77,78,22].

3.5.1.1 Tampering of devices

The attacker can extract patient health information by intercepting their wireless channels, which they can subsequently modify partially or completely before sending it back to the original recipient [29]. Such an attack aims to alter the accuracy of the information delivered messages in order to further his own objectives, which may cause doctors to make poor decisions that may endanger patients [20,85]. The adversary can construct, modify, or resend communications that have already been transferred between valid entities in order also to create an illegal effect or acquire unauthorized access [13]. Attackers can tamper with devices by exploiting some firmware vulnerabilities to install malware that then allows them to take control of the device [26] or even fully or partially stop their functionality [22,77,78].

3.5.1.2 Side channel attack

It should be mentioned that attackers can use a variety of methods to conduct a side channel assault, such as keeping an eye on the electromagnetic activity around the medical devices and examining the timing of data transfers and power consumption [22]. Confidential information underlined may be exposed in the event of a successful side channel attack [22]. Timing Attacks are a type of side channel attack in which an attacker looks at the required time for the cryptographic algorithms to complete their computations in an effort to compromise a cryptosystem. Additionally, a timing attack is a type of security exploitation in which an attacker identifies security flaws in the network or computer system as a whole. Additionally, medical devices that use OpenSSL are also the subject of timing attacks [26]. Using the “time stamping method” for packets of delay-sensitive applications may render this attack ineffective. This claim, however, ran into a difficulty with entity time synchronization [26]. Because IoMT embedded systems have relatively limited physical qualities, side channel attacks might happen. Additionally, they are utilized to find the secret key utilizing electromagnetic analysis,

differential power consumption, and power consumption. In fact, IoMT devices with physical unclonable functions (PUFs) can defend against a variety of implementation assaults. Attackers can monitor electromagnetic activity around medical devices to collect sensitive data using a variety of side-channel approaches, including data transfer timing and power usage analysis [26].

3.5.1.3 Tag cloning

In tag cloning, the attacker can copy the data from an existing tag [81] or use data gained from a successful side channel assault to carry out the attack [22]. The cloned tag, for instance, might be used to access unlawful buildings or data, including patient confidentiality. RFIDs can be copied by attackers using low-cost tools [26]. Combining cloning and spoofing attacks to launch a more complex assault [86] against a medical system or device is possible. While spoofing attacks exploit the falsified data to obtain unauthorized access, cloning attacks repeat the spoofed data [87].

3.5.1.4 Sensor tracking

Attackers can use real-time location service devices to obtain patient location during this type of attack, which is against patient privacy and their confidentiality of their data as well [77]. In reality, an attacker could be able to track the movements of the IoMT devices. This exceedingly risky attack involves intercepting and studying network traffic patterns in an effort to deduce vital information. This is because the operations of IoMT devices may potentially give sufficient information to allow an enemy to purposefully injure the medical equipment. Traffic analysis can more precisely be utilized to target specific data that can be used to create or enable fresh social engineering assaults [21, 22]. The patient's genuine identity can be determined by analyzing this trace in addition to their personal data. Therefore, learning a patient's data could compromise their right to privacy and even endanger their life [21].

3.5.1.5 Insertion of forged nodes

An attacker can introduce a fake or malicious node between the real network nodes in the IoMT network in order to obtain access and further control [22].

3.5.2 Network

The network layer has the responsibility of distributing and routing the content to the destination as well as network addressing. Delivering material, discovering content, directing content to its destination, and network addressing are also executed in network layer [22,26,77,81].

3.5.2.1 DoS/DDoS

Denial of Service Attacks (DoS): DoS attacks are initiated and launched in order to interfere with the availability of a specific medical IoMT system or device, preventing legitimate patients from receiving the right medications and preventing nurses and doctors from accessing medical data and records [21]. That aims to prevent the providing of time-critical operations or restrict access to facilities and assets that have been approved [94, 95]. Depending on the service being supplied, time-critical can be measured in milliseconds or hours. This might be accomplished by sending a large number of requests to the IoMT edge network, which has limited resources, clogging the available bandwidth [13]. Distributed Denial of Service Attacks (DDoS): These attacks can also be launched simultaneously from numerous different countries and regions of the world. This could have a much bigger effect on the availability of medical devices and systems, which could have a bad effect on patients' lives if timely responses aren't possible [21]. DDoS leverages more compromised nodes to flood the system, making it more challenging to pinpoint the attack's original source [82] Attackers can launch a variety of DDoS attacks using automated methods like botnets, which are made up of infected IoT devices (such as Telnet and Mirai). A vast network of compromised nodes can be used by botnets to perform a far-reaching DDoS attack on other devices. Due to the widespread use of unsecured IoT devices, a large-scale DDoS attack using IoT devices was successful in 2016 [26].

3.5.2.2 Rogue access

Here, the attacker creates a fake gateway, entices honest people to connect, and then intercepts network traffic to reveal the transmitting data [21, 22, 77, 79]. The SANS Institute claims that this attack can be carried out using free software and that it cannot be quickly identified because a forged gateway may conceal its existence [21].

3.5.2.3 Eavesdropping

Eavesdropping attacks depend on acquiring sensitive information. [20, 21]. A cyberattack that uses unsecured network connections to deliberately obstruct two entities' ability to communicate, such as cellphones or sensor nodes. In order to obtain important information, the attacker listens to the conversation in secrecy. Later, the attacker will utilize this knowledge to pose as the claimant. Eavesdropping operations are challenging to identify because they don't disrupt normal network transmissions [13]. In order to successfully gather the data being transferred through hardware devices, the attacker must first identify and intercept the relevant hardware devices. The information collected illegally can be applied to a variety of threats. Although encryption can be used to overcome this issue, strong encryption is not always possible due to a lack of processing power and memory, especially with low-powered IoMT

devices [22]. The drawback with eavesdropping is that it is one of the simplest techniques for attackers to gather data from sensors. Vital signs from a patient, for instance, may be intercepted during transmission. Thusly obtained data can be utilized to launch a variety of assaults. These risks could lead to the loss of private information, including physiological data, as well as information about the medical device, including the kind of equipment the patient is connected to. They may also support other types of assaults. There are two kinds [29] of eavesdropping:

- Active eavesdropping: A hacker actively gathers information by posing as a helpful entity and addressing queries to emitters.
- Passive eavesdropping: A hacker can intercept content by listening to the network's message transmission.

3.5.2.4 Man in the middle (MiTM)

The adversary controls and monitors the communication between two legitimate parties while changing the transmitted data [21]. This enables successful capturing of handshakes by allowing third parties to listen in on Address Resolution Protocols (ARP). If it manages to catch it, it utilizes it to steal encryption keys and gain unauthorized access to a system and medical records [126]. All communications sent between the two parties can be captured and new ones can be added [29]. This attack is one of the main authentication attacks. It may be active or passive. When the attacker intercepts and reads the messages sent back and forth between the two entities, it is regarded as a passive attack. On the other hand, if the attacker is able to change, manipulate, or otherwise modify the sent data or information without the awareness of any of the devices, it is regarded as an active attack [21]. It is considered as a life-risk attack, since IoMT sensing devices send and receive data, hence any alterations made to the data during transmission could result in abuse (for example, pharmaceutical overdose) [93]. A similar flaw that enables man-in- the-middle attackers to remotely compromise the device and eavesdrop on communications between the transmitter and devices attached to it has recently been discovered in St. Jude cardiac devices [26].

3.5.2.5 Sybil attack

In order to secure the privacy of any patient, the MAC and IP addresses must constantly change to avoid any potential identity disclosure, denial of service, or spoofing attack. As a result, certain new methods must be developed to address the issue of excessive memory space. As a result, each patient should be given a selection from a pool of certified pseudonyms that have been issued by a certificate authority [88, 89]. The most popular attack is the Sybil one [127]. The pool of pseudonyms can be used to send fake messages to a datacenter while posing as being for different patients. This involves false traffic jams or false notifications that compel

hospitals to react to a made-up incident. The primary goal of the authorities is to ensure that identities and any sensitive data linked with them are protected and validated throughout any communication attempt. If there is a problem, the system administrators must take action, but doing so necessitates knowing who the user is (digital forensics). This implies that privacy and digital forensics do, in fact, trade off. One of these security methods makes use of a message authentication algorithm like the cryptographic keyed hash function, or HMAC, to ensure data integrity and source authentication [21]. This kind of assault typically targets WSNs. The victim node can carry out a single operation repeatedly thanks to a node in the network system that grants it several identities. The victim node will transfer data through the infected nodes, exposing the sensitive data because the attacker has several identities in the WSN [77].

3.5.2.6 Sniffing attack

Sniffing attacks, can be used to enter into the system after blocking the accurate and correct message supplied by a genuine user [20]. As a result, this could have intercept unencrypted medical data packets being transmitted and expose their contents, including passwords and the medical status of the patients. One of the best examples of network monitoring software is Wireshark [21]. The attacker tries to steal data in network traffic using sniffing tools or programs in order to gather information that will be valuable in future attacks [22, 77].

3.5.2.7 Routing attacks

This type of attack has an impact on the routing of messages or data. In this type of attack, the attacker may spoof, misdirect, redirect, or even drop the packets at the network layer [83].

3.5.3 Application

Attacks typically aim to get unauthorized access to sensitive user data at the application layer, which ultimately violates user privacy. Attackers typically use application layer services and apps that are vulnerable to software and hardware flaws (such as buffer overflows and code injection). Along with these assaults, other malware types including worms, viruses, and trojans frequently pose a threat to applications and services. Additionally, other harmful applications such as malware, keyloggers, rootkits, adware, and others frequently compromise users' privacy [22, 77].

3.5.3.1 Session hijacking

Attacks known as "session hijacking" are frequent in RESTful-based IoT systems. Some IoT devices' handling of session connections at the web interface level makes them vulnerable to session hijacking, in which an attacker can seize control of the session data [22, 26, 77, 79, 80].

3.5.3.2 Cross-site scripting (XSS)

By incorporating malicious scripts into online pages (such as web control pages) to get around access control, cross-site scripting attacks take advantage of programs [22, 77]. Such attacks are possible on cloud-connected IoT devices' web interfaces [26].

3.5.3.3 Cross-site request forgery (CSRF)

When a web application is subjected to a CSRF assault, the attacker forces the end user to carry out undesirable actions, which might have disastrous consequences like disclosing user credentials [22, 77,79]. Without the user's knowledge, the CSRF induces the end user into acting in a certain way on a susceptible application. If improperly configured, the IoT layer's web interface is susceptible to CSRF attacks [26].

3.5.3.4 SQL Injection

This kind of attack is generated from an entity that can be legal or can authenticate with the system. By producing a message with fake information and transmitting it to the doctors and the hospital's databases, this assault has serious consequences on the IoMT systems and ultimately results in the death of patients. For instance, an attacker could introduce false update script system where adversaries can mimic a legitimate server for system backup, so this would allow a given adversary to gain unauthorized access to any IoMT device and might introduce a backdoor [91]. Additionally, the attacker injects the incorrect message or code which can have harmful consequences on the IoMT system and result in fatal accidents [90]. The strategy behind this attack is to block legitimate users from sending true messages and to flood the network with bogus information instead. Messages should be verified in order to ward off such an assault [21].

3.5.3.5 Brute force

Brute force attacks is an attempt to guess inputs such as passwords by attempting every conceivable combination [26, 92]. Such an attempt seeks to obtain patient credentials and sensitive medical data for fraud [21]. Remote patient medical sensors are not the only targets of this attack, which affects the majority of the targeted equipment [20]. Due to the majority of IoMT devices in medical networks having less computing capabilities, a simple brute force attack can easily compromise the device's access control and create doors for attackers to further compromise the network, by infecting the devices with malware [13].

3.5.3.6 Ransomware

All of a system's data is encrypted by ransomware, which demands payment in order to restore the infected machine. Ransomware may potentially start on a single compromised victim machine and then spread over the entire network if the proper security settings are not put in place [22,79,80,84].

3.5.3.7 Phishing

In a typical phishing attempt, an attacker poses as a trustworthy individual or organization in an effort to get access to personal information, including user credentials and credit card information. When a victim accepts an email or email attachment, the attacker acquires sensitive information. Email is a very typical medium for these types of phishing attacks [77,79,80]. However, phishing is just a section of a whole list of attacks that might happen in IoMT environment, so we must secure the entire IoMT ecosystem, not simply specific technology related to one layer [22, 77].

3.6 Compromise level

The area of the IoMT environment that has been breached is identified in this category. The levels of compromise are the following:

3.6.1 User

Unauthorized user access, stolen credentials, user account hijacking, etc. are examples of compromises at the user level.

3.6.2 System/App

This involves modifying the IoMT application or system-level program to make it impossible for the system to be used for what it was designed to do.

3.6.3 Hardware

This covers any actual loss of hardware, actual tampering with hardware, or actual IoMT hardware- related attacks.

3.6.4 Network

Compromises a whole network of an organization with catastrophic consequences. A user can gain access through a previous compromised level.

3.7 Impact

The impact of an attack is a significant factor as of the reaction time. For example, if we are talking about a life-risk incident, then the reaction must be immediate.

3.7.1 Life risk

If a gadget used to monitor a critical illness or treat a patient is attacked, its ability to do its job may be hindered.

3.7.2 Brand value loss

Brand value loss may result from any material or immaterial loss caused by an attack on the organization's integrity.

3.7.3 Data disclosure

If a breach is successful, patient data may become available to the public, which is against the law. In 2015, about 38% of healthcare breaches were data breaches [26].

3.7.4 Monetary value

After a system has been compromised, the sector will eventually need to retrieve data hardware and handle damage control. Each of these procedures requires additional funding, which has an influence on the organization's finances. Misinforming is common in monetary value impact and may result from attacks like man- in-the-middle and sinkhole. It's estimated that 58% of healthcare organizations lack a procedure for correcting such inaccurate information [26].

3.7.5 Disruption

The system's availability is impacted when proper operations or access to medical data are interrupted, which could have fatal results. An example of an assault designed to disrupt information is the DoS attack [26].

3.8 Damage range

Damage range is defined by 2 combined factors in our taxonomy. Also damage range defines the countermeasures that need to be taken and the time of reaction. A large damage range needs sooner reaction than small or moderate (the soonest one). We have divided below all the possible combinations (Figure 11-Figure 19) for each level.

3.8.1 Small

Impact [Brand Value Loss] or [Monetary Value] X Compromise level [User] or [System/App] (Figure 11)

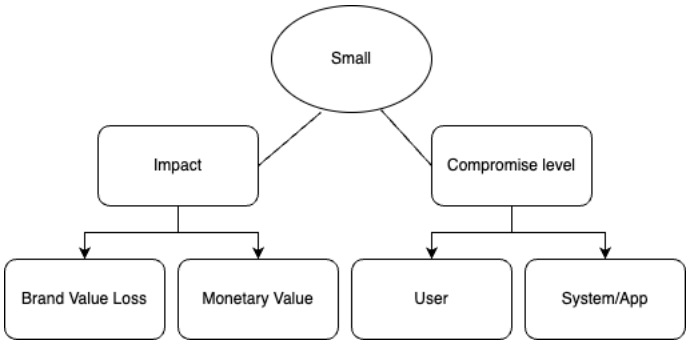

Figure 11. Small damage range 1.

Impact [Denial of Service] X Compromise level [User] (Figure 12)

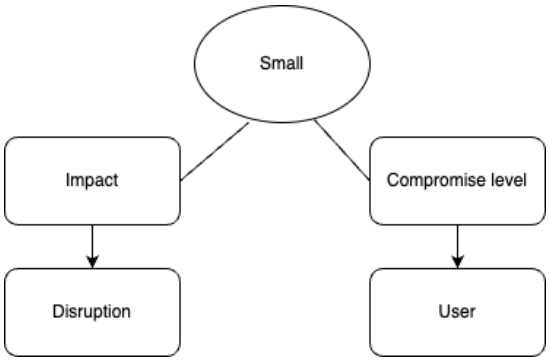

Figure 12. Small damage rage 2.

3.8.2 Moderate

Impact [Data Disclosure] X Compromise level [User] or [System/App] (Figure 13)

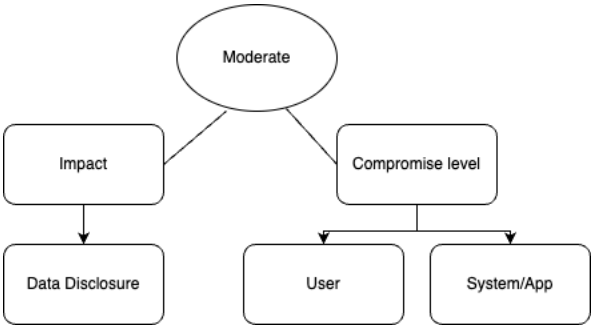

Figure 13. Moderate damage range 1.

Impact [Denial of Service] X compromise level [System/App] (Figure 14)

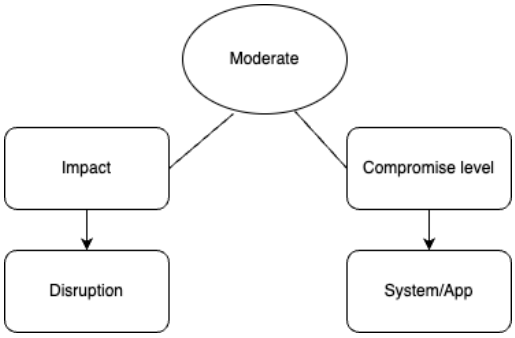

Figure 14. Moderate damage range 2.

Impact [Brand Value Loss] or [Monetary Value] X Compromise level [Hardware] (Figure 15)

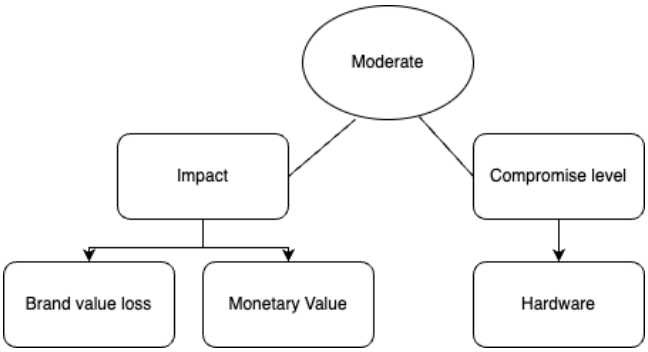

Figure 15. Moderate damage range 3.

3.8.3 Large

Impact [Life Risk] X Compromise level [User] or [System/App] or [Hardware] or [Network] (Figure 16)

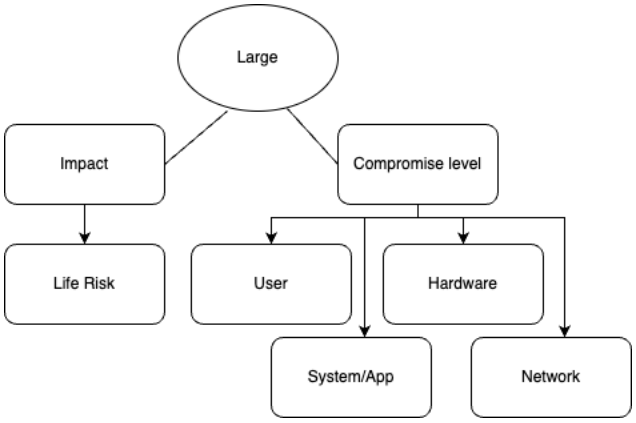

Figure 16. Large damage range 1.

Impact [Data Disclosure] X Compromise level [Hardware] or [Network] (Figure 17)

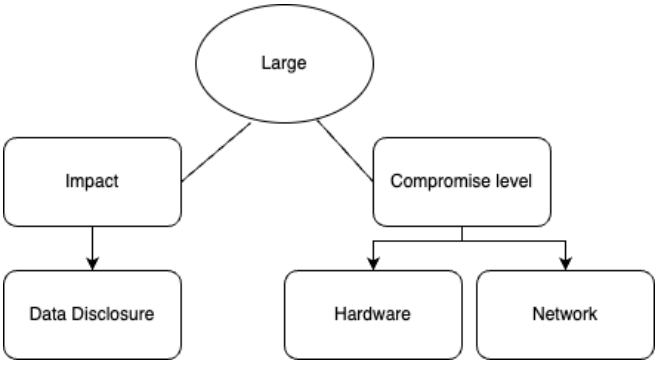

Figure 17. Large damage range 2.

Impact [Denial of Service] X compromise level [Hardware] or [Network] (Figure 18)

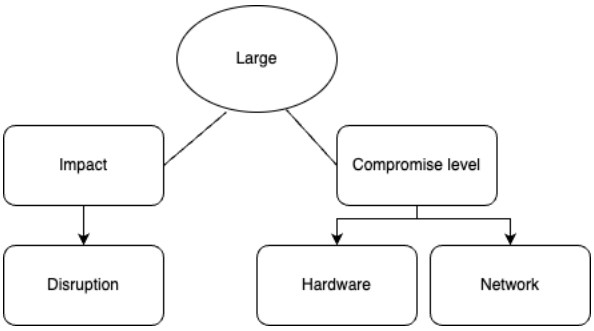

Figure 18. Large damage range 3.

Impact [Brand Value Loss] or [Monetary Value] X compromise level [Network] (Figure 19)

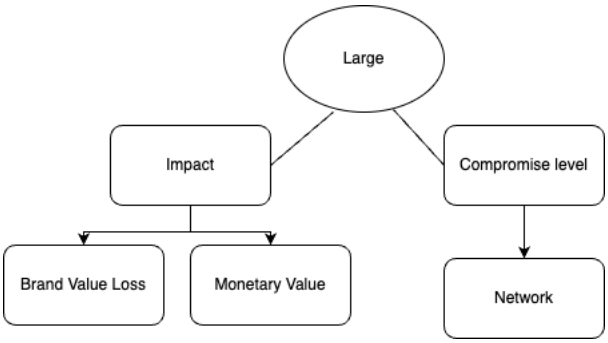

Figure 19. Large damage range 4.

3.9 Countermeasures

IoMT transmits data gathered from the human body to the medical server through wireless communication and the internet. As a result, the data in the various layers of the IoMT system are vulnerable to cyberattacks, which can compromise patient privacy and endanger their life. To prevent, recognize, and mitigate these assaults in real time, security standards must be met. At this section we present the primary IoMT security criteria. We categorize security countermeasures against the mentioned risks to IoMT edge networks that have been found in the literature. Based on the security goals that they achieve within IoMT edge networks and the

data level that needs to be ensured, the examined countermeasures are divided into categories [13].

3.9.1 Confidentiality

Confidentiality ensures that private information is not shared with or obtained by unauthorized parties [13]. In the IoMT edge network refers to preventing the disclosure of patient medical information to unauthorized parties who could hurt the patient or use this information inappropriately. This information is exchanged with a therapist, a doctor, or other medical professionals. An adversary, for instance, could interfere between the sender (such as a medical IoT device) and the receiver (such as a smartphone-gateway) in order to intercept the transmitted medical data and access unlawful information if the confidentiality of the communicated data is not maintained. There are many ways to preserve secrecy, from physical security to cryptographic techniques that render data unreadable [13]. Health information about patients must be collected and stored in accordance with ethical and legal privacy rules, such as GDPR and HIPAA, so that only people with permission can access the information. Adequate safeguards for the confidentiality of patient health information must be adopted in order to prevent data breaches. It is crucial to take these precautions because if cybercriminals sell the data they have obtained, patients may suffer not only from privacy violations but also from potential financial and reputational harm. Article 5(e) of the GDPR states that personal data should be deleted after processing and when it is no longer necessary, with few exceptions for archiving, scientific, historical, or statistical reasons (Article 89). HIPAA, on the other hand, places no limitations on how long patients' data may be stored. While healthcare providers who are in compliance with the GDPR are required to obtain the explicit consent of EU patients before sharing their protected health information (PHI) with other providers, medical service providers who are in compliance with HIPAA are permitted to do so without the patients' consent [10, 121]. Only authorized personnel will be able to access the medical information thanks to confidentiality, which prevents access by unauthorized individuals [22].

3.9.1.1 Security threats to data confidentiality

IoMT edge networks are made up of resource-limited IoT devices that prevent the use of resource-demanding cryptographic solutions (like data encryption/decryption) that ensure a high level of data confidentiality, leaving the network open to threats aimed at the confidentiality of the exchanged or stored data [13]. An opponent may, for instance, eavesdrop on conversations taking place within the IoMT edge network, follow communications, and read the information included in the transmitted packages [100]. A wearable sensor that wirelessly communicates a patient's vital signs to an IoMT gateway (such as a patient's smartphone) can

be passively intercepted by the adversary, who can then extract sensitive data (for example, by traffic analysis) and utilize it for malevolent purposes [101]. Furthermore, interrogation attacks, which may be viewed as a form of impersonation, might jeopardize the confidentiality of data [97]. A hostile actor may appear as a trustworthy entity and send queries to other entities with the sole intent of disclosing users' confidential information [102].

3.9.1.2 Ensuring confidentiality

The management of IoMT devices' confidential data generated, stored, communicated, and processed within the IoMT edge network environment requires specific attention. Lightweight encryption techniques have been established using the ISO/IEC 29192 [111] requirements in order to protect data confidentiality in resource-constrained IoMT devices. There are many simple lightweight cryptographic protocols that can create secure connections between restricted IoMT devices, including the medical sensors and nodes [106]. Examples include symmetric key ciphers (also known as block and stream ciphers) and hash functions. However, the key distribution issue affects symmetric key ciphers. For instance, IoMT devices' fixed, preconfigured keys are susceptible to theft. Furthermore, since many users, such as elderly individuals, are unable or unwilling to configure secure secret keys or update them frequently, secret keys should be updated automatically. According to [112,113,114], shared keys should be generated with little computational and energy cost, high unpredictability, and high agreement between the two communicating entities. As a result, IoMT devices face an issue with the production of shared keys, and numerous efforts have already been presented to address it. There are still unresolved challenges in balancing the requirements of public key cryptography with the restrictions of IoMT devices, despite the fact that symmetric key cryptography is more lightweight and ensures privacy preservation for resource-constrained IoMT devices [13]. One aspect that impacts how effectively PKI technology is adopted in healthcare networks, for instance, is the degree of complexity of the certificate path processing in a PKI infrastructure [13].

3.9.2 Integrity

The goal of the data integrity requirement for IoMT healthcare systems is to ensure that the data have not been damaged in any way throughout the wireless transmission [10], including individual medical records, health summaries, clinical notes, and test results. Particularly, the adoption of cutting-edge IoT technologies in the healthcare industry has increased the reliance on networked data, and healthcare organizations are now more aware than ever of the value of data integrity [13]. In addition to data integrity, the ideas of device and software integrity have received attention in the context of the IoMT edge network. The reliability of the wearable or

implanted sensors used in the IoMT edge networks is also crucial for their effective adoption in the healthcare industry. IoMT devices are vulnerable to physical attacks that aim to compromise device integrity since they often operate in untrustworthy environments. In addition, a crucial component of guaranteeing security in the IoMT edge network is the integrity of the software that is currently executing on the medical devices (such as operating systems and applications) [13]. By taking advantage of the wireless network's broadcast feature, attackers might access and alter patient data, which could have serious consequences in life-threatening situations. The ability to spot suspected illegal data distortions or manipulations is crucial for ensuring that the data have not been compromised. Therefore, it is necessary to include suitable data integrity mechanisms to stop hostile attacks from changing sent data. We suggest a technique to ensure that someone other than the individual engaged (i.e., doctors or nurses) does not change the medical data by maintaining the integrity of the information, which prevents the administration of ineffective medication [29]. Additionally, it is important to guarantee the data's integrity, which means it can't be tampered with, while it's housed on medical servers. According to Article 5(d) of the GDPR, healthcare providers must take the necessary steps to maintain the accuracy and timeliness of patient data. Inaccurate personal data must also be changed or removed as soon as possible. The GDPR also places a strong emphasis on the "accuracy" of the data, allowing data owners to ask service providers to correct any erroneous data. The requests must be answered by the providers within one calendar month. Similar to this, HIPAA mandates that providers of medical services take the appropriate steps to guarantee that any PHI kept in the systems cannot be changed without authorization [10].

3.9.2.1 Security threats to integrity

Because the attacker intervenes in the communication between the two sides and has the potential to modify the shared data covertly, a Man-in-the-Middle (MItM) attack is one type of attack that can compromise the integrity of IoMT edge networks [115,116]. For example, the IoMT edge network's acquired medical data can be sent to a distant server or retained locally in the internal memory of the wearables. In the case of transmission, the attacker can eavesdrop on and alter the sent medical data, jeopardizing its integrity. Additionally, the authors in claim that the malicious node injection attack is the most severe physical assault since it not only disrupts the services that are being given but also changes the data that is being stored. Physical attacks on the devices themselves are another prominent attack method that successfully aims to undermine the integrity of IoMT devices. For instance, a malicious attacker with physical access to an IoMT device could modify its structure to affect how it behaves. Finally, the absence of portable malware detection tools for IoMT devices makes it possible for hackers to also undermine the integrity of medical equipment. For instance, by running malicious code on

an IoMT device and taking advantage of its networking software and hardware's security flaws, an attacker can damage the device [13].

3.9.2.2 Ensuring integrity

The integrity of transmitted data is ensured in by the use of symmetric cryptography and attribute- based encryption (ABE) in the context of an IoMT edge network [117]. A random symmetric key (RSK) that is encrypted with ABE is used to encrypt the transmitted communications. The RSK and the message are decrypted if an IoMT device possesses the appropriate secret key that complies with the ABE access policy. The device attributes set, which stand in for the user's privileges, are attached to the secret key. In this situation, there is the possibility to omit the entire message from encryption and only encrypt the downloaded RSK, increasing communication range and decreasing encryption expense. Elliptic curve cryptography (ECC), on the other hand, is a different process that is used to encrypt the public key utilizing a smaller key size than RSA [118] and is more computationally lightweight. Practically all communication protocols include traditional cryptographic security guarantees such data integrity. However, virus attacks and node compromise are not intended to be included in such protection by the cryptographic security built into communication protocols. Therefore, in addition to data integrity, software integrity is viewed as a crucial component to ensuring the security and privacy of the IoMT edge network.

3.9.3 Availability

Data and services must be available when needed to the appropriate users. In the context of an IoMT edge network, it is crucial to guarantee that device and network resources are accessible when a patient need uninterrupted medical care [115]. For example, a doctor must always have uninterrupted access to all patient clinical records, wherever they may be. Additionally, it's critical to act quickly in an emergency so that the doctor can treat the patient or take preventative measures. A different option would be to switch to a different network node, and the network and system design may permit this redundancy [29]. If DoS attacks take place, the medical servers and devices' services and data will no longer be available. Any unavailable information or services could result in potentially fatal situations, such as failing to send out a timely notice in the event of a heart attack. Since data availability to users and emergency services must be guaranteed, healthcare apps must be always-on to account for the probability of availability loss [13]. Medical service providers are required by Article 32 of the GDPR to have the capacity to promptly restore availability and access to personal data, including by implementing preventive security measures and DoS attack defenses. Furthermore, under Article 17 of the GDPR,

patients in the EU have the right to ask that the medical service providers delete any records of them; this right, known as the ”Right to Be Forgotten,” is not mandated by the HIPAA [121].

3.9.3.1 Security threats to availability

The constraints and drawbacks of the current centralized cloud-based healthcare systems are being overcome by IoT technology, which is being deployed in a growing number of healthcare applications. Healthcare systems, where IoMT devices are widely used, are confronted with resource and computing power limitations [108], which make it difficult to maintain the availability of the services offered. In reality, the IoMT edge network's limited resources can make it extremely vulnerable to DoS. Different types of DoS attacks, such as tampering, jamming, battery depletion, collision, congestion, and IoT-botnet assaults, can be applied to different network tiers and have varying effects on the IoMT edge network [119]. Tampering is more specifically defined as the change of sent data that prevents the IoMT edge network from operating normally [106]. Due to the nature of the inadequate and insecure wireless communication in the IoMT edge network environment, tampering attacks are difficult to detect. Additionally, jamming attacks rely on the massive amount of delivered messages to overburden processing or communication resources, preventing IoMT devices from enjoying the services offered normally [106]. An IoMT edge network's unavailability renders it immediately ineffective for providing real-time healthcare services and may jeopardize patient's safety [13]. A patient in a critical condition may not receive the attention they require in an IoMT-enabled healthcare alert system, putting their life in danger. This can happen if the communication channels within the IoMT edge network are blocked. A battery draining attack against an IoMT device that targets the battery consumption of the resource constrained IoMT device may lead to the same outcome. An adversary that sends the target IoMT device intentionally bogus or erroneous messages can carry out a battery drain assault [98, 99]. Additionally, two nodes simultaneously transmit data on the same frequency channel during collision assaults, leading to identification mismatch at the receiving end. This results in the IoMT edge network wasting resources by discarding malformed received data packets and retransmitting the identical packets [98]. Additionally, a channel congestion attack is carried out by sending a large number of pointless messages, which results in excessive channel traffic and the inaccessibility of time-related IoMT services and data. The availability of IoMT edge networks can potentially be a target of Distributed Denial of Service (DDoS) assaults, where an attacker can overwhelm the target device (such as a gateway) by flooding it with numerous requests using an IoT botnet. Because of the limited resources of its devices, it is important to note that the IoMT edge network is more susceptible to DoS assaults than the Cloud platform in an IoMT-based healthcare system [13].

3.9.3.2 Ensuring availability

The availability of the connected medical devices should be guaranteed due to the importance of the data in an IoMT edge network environment. IoMT devices are subject to resource and processing power limits, as was previously described [108]. The distributed Strength of Crowd (SOC) protocol may be appropriate for IoMT devices with limited resources [120]. Despite the possibility of blocking a significant percentage of the available bandwidth, this protocol ensures that messages reach the receiving nodes. SoC focuses on tricking the enemy by sending deception packets from genuine devices to the network, confusing the jammer as to which devices are the actual ones. The DoS attacks are another form of attack that needs to be handled carefully in terms of availability. Due to the lightweight and low computational nature of IoMT devices, adversaries may influence them to overwhelm the edge network's communications and services with a large volume of request messages, which could also cause the devices' batteries to discharge. Adopting a simple pattern/behavior recognition algorithm with a notification system in order to identify anomalous actions could be a solution (posing as DoS attacks care). It is important to note that more research should be done to address the issues brought on by the limitations of IoMT devices in order to address the dangers that jeopardize the availability of the crucial services offered by an IoMT edge network environment.

3.9.3.3 Resistance to DoS attacks

Attackers can utilize high-energy signals, such as jamming attacks in the physical layer [122], to prevent the wireless network from functioning properly. Many solutions, including evasion defense and competition tactics, have been put out to protect and self-repair the network against such attacks, however they are all still in the early stages of study [122]. Due to the mobile and dynamic nature of wireless networks, much study is needed to create solutions to defend the system against DoS assaults for real-time IoMT healthcare systems [123].

3.9.4 Non-repudiation

Non-repudiation ensures that any party involved in the healthcare application cannot dispute the sending or receipt of patient health-related data [29]. One patient's sensors may be used to extract data, which may be sent, but the patient may later claim the data do not belong to him. Alternately, a licensed developer may upgrade the software in a few sensors and then contest its accuracy. There is a need for a method of resolving conflicts when an entity disputes prior agreements or specific acts that were permitted. To resolve such disagreements, a particular process including a reliable third party is frequently required.

3.9.4.1 Ensuring non-repudiation

A method of resolving issues referring to non-repudiation is crucial when disagreements originate from an entity that contests prior obligations or conduct [13]. Auditing, which securely stores all the operations carried out by or on them, is a frequently used method in IoMT devices to handle these situations. Auditing is the inspection of changes in the system and access to the patient's medical data via the verification of log files, which are historical records of the hardware and software operating status. The audit allows the detection of abnormal activities and possible breaches. However, the management and exploitation of this type of information are delicate in practice due to the large quantity and heterogeneity of logs generated by the various medical and network equipment [29].

3.9.5 Authentication

3.9.5.1 Entity identification

The procedure by which one communicating entity is confident in the claimed identity of another entity participating in the contact and that the latter has actually taken part is known as entity authentication or identification. Effective user authentication techniques are needed since only patients and medical personnel should have access to the data kept on personal servers, either temporarily or permanently [123]. In the IoMT healthcare systems, personal servers should also provide emergency access to the data if patients are experiencing life-threatening circumstances, such as a stroke or a seizure. The usage of biometrics, which is particularly applicable in IoMT healthcare systems because the majority of biometrics can be easily acquired from medical and healthcare devices worn by or implanted in human bodies, is a common method of user authentication at the personal server level [124].

3.9.5.2 Message authentication

Message authentication, on the other hand, is the procedure used to confirm that a particular entity is the original source of data that was generated in the past. Lightweight authentication algorithms are becoming more popular these days since many IoT devices lack the memory and processing capacity necessary to carry out the cryptographic operations needed by conventional authentication protocols.

3.9.5.3 Device authentication

Before receiving data sent from the medical equipment and sensors, a personal server (such as a smartphone) must carry out authentication. For the confidentiality and integrity of data, a device authentication mechanism should be able to establish secured/encrypted

communications. Device authentication must be incorporated in any IoMT healthcare systems since false information from malicious devices about patients' physical status could have detrimental effects on the clinical diagnosis and care decisions. Device authentication is symmetric between personal servers and devices, but as personal servers frequently have more computing power and capability than medical devices and sensors, most of the calculation should be done there [10, 125].

3.9.5.4 Security threats to authentication

One of the fundamental security requirements of an IoMT-based healthcare system is authentication. The standard PKI-based authentication solutions are ineffective and non-expandable due to the IoMT devices' ubiquity. Additionally, adversaries target a system's weak authentication to access resources based on users' identities without having valid credentials. The initial phase of a forgery attack focuses on fabricating an identity so that the malicious user can be identified. The attacker then sends false data to other entities in an effort to scam them [106]. Sybil attacks, in which an IoMT device assumes many false identities, can also be detrimental since they enable malicious devices to mimic other trustworthy devices in the IoMT edge network. For instance, the rogue node can link to several other IoMT devices to increase its effect and potentially trick the system into making false inferences. Device cloning/replication attacks differ from sybil attacks in that each device only has one identity. In this kind of attack, an adversary gains control of a sensor device and obtains encrypted data that is then utilized to make a sizeable number of network clones and carry out other assaults that compromise authentication and security goals [96]. When location-based authentication methods are not used throughout the authentication process, the malicious intent to expel devices from the same location is successful [96]. Finally, IoMT edge networks may also be the target of impersonating assaults [97]. The two types of masquerading attacks are as follows: either an attacker poses as a legitimate user in order to implant rogue devices and obtain access to the services that IoMT devices offer, or an attacker is purportedly disguised as an IoMT device in order to offer fake services to users. The last scenario is risky for the healthcare industry because many patients depend on the IoMT devices' services for their survival [106].

3.9.5.5 Ensuring authentication

A crucial requirement for IoMT security is authentication. There are many different authentication protocols and methods, however the resource limitations of IoMT devices present one major issue: the use of robust authentication methods with these devices' low battery and processing capacity. Thus, for IoT networks like the IoMT edge networks, a lot of focus should be placed on lightweight authentication systems [100,106-110]. For instance, an

improved certificate-based DTLS handshake protocol is suggested as an authentication method in [105], with three key changes: a) pre-validating the certificates at the IoMT nodes to reduce the tasks executed in the constrained devices; b) forwarding resumptive sessions to reduce the transmission and processing overhead; and c) delegating the handshake procedure for devices that cannot execute a certificate-based protocol. It's important to note that when these changes were put in place, using certificates seemed less burdensome. A simplified authentication and key agreement mechanism called PPAKA-HMAC and an upgraded protocol called PPAKA-IBS are also examined in [104]. For secure communications between the devices, the first one combines group key agreement with hash-based message authentication code (HMAC) and pseudonym management, and the second one employs Identity-Based Signature (IBS) as opposed to PPAKA-HMAC [104]. The first one provides security against external harmful actors and secure communication in a light-weight manner, whilst the second one offers resistance to internal malicious activity. Both are deemed suitable for IoMT device mutual authentication in real-time edge networks. There is still a lot of research being done on lightweight versions of authentication algorithms that are appropriate for IoT devices and can also be used with IoMT devices. Despite the fact that numerous authentication strategies for IoT devices have been put out by researchers, it is important to note that much work will need to be done in the future to design and create authentication mechanisms suitable for the resource-constrained IoMT devices.

3.9.6 Authorization

Authorization is the transfer of official privilege to do or be something or someone else. To put that in perspective, authorization guarantees that only authorized parties can access particular network services or resources, such as a medical IoT device or gathered patient medical data. For example, only parties with trusted expertise are given authority to carry out a certain task, such as sending commands to medical IoT devices or updating the software on those devices.

3.9.6.1 Security threats to authorization

Poor authorization procedures on an IoMT edge network may be targeted by attackers to gain access to network resources without the proper permissions. IoMT devices may be vulnerable to social engineering attacks since users may lack security knowledge and training, according to [97]. As a result, a malicious actor may mislead the IoMT edge network and pose as a reputable organization in order to gain access to a user's medical devices. In terms of medical instruments that monitor vital signs, this might put the patient's life in risk [103]. Malware attacks may potentially affect the linked IoMT devices by taking advantage of their built-in weaknesses, such as flaws in authorization systems. The infected IoMT devices can be used as

bots to launch additional attacks on other IoMT edge network devices, giving the attacker access to network services (such taking control of multiple IoMT devices) or resources (like the patient medical data that has been gathered) [13]. A typical security method for ensuring authorization is access control.

3.9.6.2 Ensuring authorization

Effective access control systems must be put in place to guarantee that only authorized individuals and devices have access to the medical servers. Since it is challenging to obtain a patient's permission or consent each time a request for data access is made, the service providers of the medical servers should offer patients selective access control, allowing them to specify which data can be shared with third parties without their permission and who has access to it. Attribute-Based Encryption (ABE), which is a type of public-key cryptography where the secret keys are produced from attributes, is a well-liked method of selective access control (i.e., received signal strength, location, and channel frequency). A set of attributes can be used to form an access tree in an ABE solution, and only sets of attributes that satisfy the tree will be allowed access to the encrypted data. Additionally, medical servers must be effective in updating access control policies. For example, many cloud security measurements call for the changing of encryption keys when updating access control policy, which results in decrypting and re-encrypting data in the medical servers and in the personal servers. Policy updates can be redundant for medical servers. Therefore, it is necessary to implement a scalable and less redundant policy updating technique in order to minimize or completely do away with the computational overheads in cryptography. A common option is two-layer over-encryption, in which the base encryption layer is required by the data owners, but a surface encryption layer (SEL) allows policy updates (BEL). Furthermore, medical servers should allow emergency access control by removing security features over patient data or by granting third parties emergency access. Proxy Re-Encryption (PRE), for instance, can be used to transform data encrypted with a patient's public key into encrypted data that can be decrypted by a third party, all without disclosing the patient's data in the process.

4

Discussion

Although the security of IoT and IoMT networks and devices is improving as the underlying technologies mature, there are still several security concerns when it comes to safeguarding patient health information. This makes defending medical services an even more difficult undertaking, especially given the diversity of technology utilized in such networks, the heterogeneity of the devices and the compact power resources. In order to create a comprehensive plan for adopting IoMT services, future initiatives should address this technical dissonance and look at the typical traits employed in medical services. To guarantee that their high standards are always reached, this will necessitate a thorough understanding of medical equipment and services.

4.1 Machine learning

One very popular study topic is machine learning, which has implications in almost every field, including network security. Numerous machine learning-based networks, including intrusion detection techniques, have recently been presented and they could be used in IoMT healthcare systems.

4.2 Deep learning

Another very important topic for IoMT cybersecurity is deep learning. Deep learning algorithms should be assessed for system security and privacy because they are increasingly being used in medical servers for illness detection. In addition, they could be used to investigate different tiers of IoMT systems for intermediate attack detection.

4.3 Blockchain

With interconnected "blocks" on the blockchain, the blockchain was first intended to secure sensitive transactional data decentralized. It might be widely applied to medical data scattered among medical servers, offering IoMT medical systems great security and privacy protection. Blockchain requires a significant number of computational resources to generate blocks, which is not feasible on IoMT devices with limited resources, however it can be used to protect cloud medical data stored in servers.

4.4 Autonomous IoMT systems

To avoid cloud-stored medical data, the next step would be an autonomous IoMT system which would make decisions based on real-time data. This has several challenges to face and limitations as well, however in the coming years it could be possible step by step, by giving robot sensors the privilege to decide about less risky medication for the patients and progressively, if succeed, taking more serious decisions based on real-time data. This would be beneficial for using only the least needed communication protocols and not cloud at all, decreasing all the risks cloud brings.

4.5 Enablers and devices as part of the IoMT taxonomy

The suggested taxonomy could be expanded and be even more specific for attack mitigation. Enablers and new IoMT devices could be part of this taxonomy as well. Combined with the communication protocols the taxonomy could result in more accurate and quick results in attacks, so the mitigation would be possible and quick as well.

In addition, medical stuff could expand the taxonomy from their perspective, underlying more possible threats to specific devices. A collaboration with medical stuff for the expansion of the IoMT cybersecurity taxonomy would benefit both cybersecurity and medicine domain in general.

4.6 Lightweight encryption and authentication

Failure to use encryption could result in data being intercepted, changed, or even permanently deleted. As a result, encryption methods -more specifically, dynamic encryption- must be used to protect the data and guarantee its confidentiality. Additionally, it is necessary to use a powerful multi-factor authentication system.

To enable the secure transmission of real-time medical data, additional lightweight security techniques are needed for authentication and encryption, particularly for smart healthcare devices with limited resources. This necessitates finding the ideal balance between the IoMT system's performance and its security and privacy features.

Lightweight cryptographic algorithms are suggested as a solution to ensure data confidentiality, integrity and availability, with source authentication and non-repudiation. Heterogeneity of the devices is already a huge challenge, as for some of them even lightweight cryptographic algorithms would be considered high-resource demanding. Key thing here is that medical data should be exchanged in real-time without any delay.

Lightweight authentication protocols in IoMT should include a hash function (with or without a key), as well as symmetric and asymmetric cryptographic algorithms. By creating an effective cryptographic algorithm for IoMT, the latency and resource requirements of the relevant computing environment would be reduced. Additionally, it's crucial to minimize the quantity and amount of messages exchanged during the authentication process.

4.7 Data minimization

According to the principle of data minimization, the IoMT services should only collect the personal health information that is essential and should only keep that data for as long as is required to achieve the goals of the services that the users are seeking. A key component of efficient data reduction strategies in the healthcare industry is reducing the total amount of patient personal data gathered.

On the other hand, the other techniques that can be used include only gathering adequate and relevant patient data and data that is in line with the intended purpose: erasing or masking unnecessary or outdated personal data and performing periodic checks to ensure the accuracy and relevance of the data that is collected. The efficient application of data reduction would also help to minimize the dangers and lower the cost of storage, as too much personal data may bring higher risks, as it is an attraction pole for attackers.

4.8 Anonymization

By removing or encrypting the identifiers that link a specific person to stored data, data anonymization refers to the process of securing confidential or sensitive information. For example, one can use a data anonymization procedure to keep personally identifying information like a person's name, social security number, and address while obscuring the source of the data.

4.9 Medical staff awareness

There is a significant level of mistrust among patients who are expressing grave worries about their privacy, particularly considering the recent hacks that exposed patient data and confidential medical information. Therefore, building trust is essential and should be given top importance. In addition to safeguarding data and guaranteeing privacy and security, it's critical to keep IoMT operations at a high degree of precision to prevent mistakes that could result in avoidable loss of life.

The improvement of patient safety and wellness depends on medical staff members continuously receiving training in information security principles in order to provide security and appropriate protection for IoMT applications and private patient data. A budget must be set aside to increase medical staff awareness, conduct training, and improve their technical knowledge in order to recognize any potential phishing, social/reverse engineering or other attacks that may put in danger a patient's life. In order to secure, manage, and safeguard the privacy of stored sensitive secret medical data and information, the IT employees should also receive additional specific training.

4.10 Zero-day attacks prevention

IoMT devices are very likely to be abused by zero-day vulnerabilities because to their inherent ubiquitous nature and rapidly evolving threats, which raises concerns about regularly upgrading devices to patch potential vulnerabilities before hostile attackers try to exploit them. On the other hand, attackers are constantly seeking for gaps or weak points to exploit. For instance, the outdated programs that are commonly found in the application layer are the most exposed to security attacks. Similar to this, healthcare system providers rarely update physical IoMT devices with the latest software, leaving end-user devices open to attack. As a result, healthcare service providers should often update IoMT devices and applications to maintain high availability and avoid zero-day attacks.

4.11 Mobility

Key question is the high mobility of the IoMT devices. If a patient uses a wearable heart rate monitor which connects to the internet via Wi-Fi, then every time the patient changes a location and connects to a new network, their IoMT device security depends on the environmental security configurations.

5

Conclusions

Our research focused on cybersecurity taxonomies, analyzing the literature and extracting useful information. We studied the background of IoT and IoMT as part of the IoT, their architecture and their vulnerabilities. Especially in IoMT, we studied its communication, its devices and all the challenges it faces in cybersecurity. The existing taxonomies we studied tried to mitigate the impediments in cybersecurity, some of them have serious strengths and other are quite old so they cover only basic and known attacks.

After comparing the existing taxonomies, our research highlighted and addressed the primary issues, difficulties, and disadvantages of IoMT, as well as the various security measures that may be put in place to protect and secure the IoMT domains and their related assets, such as medical devices and systems. Despite its benefits, IoMT is vulnerable to a range of assaults and challenges that primarily target patient privacy as well as the confidentiality, integrity, and accessibility of medical services. It is clear from the literature evaluation in this study that security must be a key component of any IoMT system that is developed and deployed.

Although IoMT security has received a lot of attention, the corresponding standards and technical specifications are still developing and are still far from reaching the ideal maturity level. Many researchers are currently working on novel secure IoMT solutions in response to the growing demands for the security and privacy of the IoT. These solutions will provide a wide range of practical services and applications to boost the effectiveness of medical care while maintaining security and privacy in any situation. In this paper we suggested a cybersecurity taxonomy for IoMT, from which derives a holistic approach of attack mitigation. We included the nature of the attack, the attacker and motivation, the communication protocols that were compromised, the attack method as of the targeted layer, the compromise level, the impact, the damage range and the countermeasures accordingly. There is no other IoMT taxonomy, as of now, in the literature that focuses on all the aspects of an attack. This is the

strength of the taxonomy we propose, and it can be used either for attack prevention, to check and prepare a system, or for mitigation, after an attack takes place.

Our discussion includes suggestions for the future and challenges in cybersecurity and IoMT. it's critical to uphold a high standard of security, privacy, trust, and accuracy. Machine learning techniques, deep learning, blockchain, autonomous IoMT systems, taxonomy expansion, lightweight encryption and authentication are the components of first level solutions in the future for the IoMT. Data minimization, anonymization, medical staff awareness are temporary or short-term solutions. We need to remember that cybersecurity needs to be addressed continuously, as intruders will always try and find a new vulnerability. Zero-day attacks prevention and mobility are factors that need our attention for the future, as they dispute cybersecurity constantly.

In conclusion, the goal of this study was to provide adequate knowledge in IoT and IoMT ecosystem and highlight the demands and aspects of cybersecurity. After providing a brief comparison of existing literature, we suggested an IoMT cybersecurity taxonomy, including all the aspects of an attack, from the beginning to the mitigation. We, finally, suggested possible expansions of our taxonomy and other research trends accordingly as well.

6

References

[1] Spanakis EG, Bonomi S, Sfakianakis S, Santucci G, Lenti S, Sorella M, Tanasache FD, Palleschi A, Ciccotelli C, Sakkalis V, Magalini S. Cyber-attacks and threats for healthcare - a multi-layer thread analysis. Annu Int Conf IEEE Eng Med Biol Soc. 2020 Jul;2020:5705-5708. doi: 10.1109/EMBC44109.2020.9176698. PMID: 33019270.

[2] Lopatina, Kate & Dokuchaev, V. & Maklachkova, V.. (2021). Data Risks Identification in Healthcare Sensor Networks. 1-7. 10.1109/EMCTECH53459.2021.9619178.

[3] Matni, Nagib & Moraes, Jean & Pacheco, Lucas & Rosário, Denis & Oliveira, Helder May & Cerqueira, Eduardo & Venancio Neto, Augusto. (2020). Experimenting Long Range Wide Area Network in an e-Health Environment: Discussion and Future Directions. 758-763. 10.1109/IWCMC48107.2020.9148524.

[4] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue and J. -C. Prévotet, "Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1561-1581, Secondquarter 2019, doi: 10.1109/COMST.2018.2877382.

[5] M. K. Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," in IEEE Access, vol. 9, pp. 47731-47742, 2021, doi: 10.1109/ACCESS.2021.3061710.

[6] Hasan, Mohammad & Islam, Shayla & Sulaiman, Rossilawati & Khan, Sheroz & Hashim, Aisha & Habib, Shabana & Islam, Muhammad & Alyahya, Saleh & Ahmed, Musse & Kamil, Samar & Hassan, Md. (2021).

Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3061710.

[7] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," in IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8707-8718, 1 June1, 2021, doi: 10.1109/JIOT.2020.3045653.

[8] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou and C. Tsatsoulis, "Review of Security and Privacy for the Internet of Medical Things (IoMT)," 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2019, pp. 457-464, doi: 10.1109/DCOSS.2019.00091.

[9] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou and C. Douligeris, "Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal," in IEEE Access, vol. 9, pp. 40049-40075, 2021, doi: 10.1109/ACCESS.2021.3064682.

[10] Y. Sun, F. P., W. Lo and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," in IEEE Access, vol. 7, pp. 183339-183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[11] K. Tsantikidou and N. Sklavos, "Vulnerabilities of Internet of Things, for Healthcare Devices and Applications," 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), 2021, pp. 498-503, doi: 10.1109/NICS54270.2021.9701497.

[12] Shakeel, T., Habib, S., Boulila, W. et al. A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects. Complex Intell. Syst. (2022), doi: 10.1007/s40747-022-00767.

[13] Papaioannou, M, Karageorgou, M, Mantas, G, et al. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). Trans Emerging Tel Tech. 2022; 33:e4049, doi: 10.1002/ett.4049

[14] Jahankhani H, Ibarra J (2019) Digital Forensic Investigation for the Internet of Medical Things (IoMT). Forensic Leg Investig Sci 5: 029, doi: 10.24966/FLIS-733X/100029

[15] Joyia, Gulraiz & Liaqat, Rao & Farooq, Aftab & Rehman, Saad. (2017). Internet of Medical Things (IOMT): Applications, Benefits and Future

Challenges in Healthcare Domain. Journal of Communications. 12. 240-247. 10.12720/jcm.12.4.240-247.

[16] M. Irfan and N. Ahmad, "Internet of medical things: Architectural model, motivational factors and impediments," 2018 15th Learning and Technology Conference (L&T), 2018, pp. 6-13, doi: 10.1109/LT.2018.8368495.

[17] Aman, Azana & Hassan, Wan & Hameed, Shilan & Mahmod, Zainab & Alizadeh, Mojtaba & A Latiff, Liza. (2021). IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. Journal of Network and Computer Applications. 174. 102886.

[18] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," in IEEE Access, vol. 7, pp. 182459-182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[19] Alsubaei, Faisal & Abuhussein, Abdullah & Shandilya, Vivek & Shiva, S.. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. Internet of Things. 8. 100123. 10.1016/j.iot.2019.100123.

[20] Razdan, Sahshanu & Sharma, Sachin. (2021). Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. IETE Technical Review. 10.1080/02564602.2021.1927863.

[21] A. Yaacoub, Jp & Noura, Mohamad & Noura, Hassan & Salman, Ola & Yaacoub, E. & Couturier, Raphaël & Chehab, Ali. (2019). Securing Internet of Medical Things Systems: Limitations, Issues and Recommendations. Future Generation Computer Systems. 105. 10.1016/j.future.2019.12.028.

[22] Elhoseny, Mohamed & Thilakarathne, Navod & Alghamdi, Mohammed & Mahendran, Rakesh & Gardezi, Akber & Weerasinghe, Hesiri & Welhenge, Anuradhi. (2021). Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. Sustainability. 13. 11645. 10.3390/su132111645.

[23] Rasool, Raihan & Ahmad, Hafiz & Rafiq, Wajid & Qayyum, Adnan & Qadir, Junaid. (2022). Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. Journal of Network and Computer Applications. 201. 103332. 10.1016/j.jnca.2022.103332.

[24] Koutras, Dimitris & Stergiopoulos, George & Dasaklis, Thomas & Kotzanikolaou, Panayiotis & Glynos, Dimitris & Douligeris, Christos.

(2020). Security in IoMT Communications: A Survey. Sensors. 20. 4828. 10.3390/s20174828.

[25] Janardhanan, Jeyavel & Hariharan, U. & J.MannarMannan, & Parameswaran, T.. (2021). Security Vulnerabilities and Intelligent Solutions for IoMT Systems. 10.1007/978-3-030-63937-2_10.

[26] F. Alsubaei, A. Abuhussein and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), 2017, pp. 112-120, doi: 10.1109/LCN.Workshops.2017.72.

[27] Yassine, Imad & Halabi, Talal & Bellaiche, Martine. (2021). Security Risk Assessment Methodologies in The Internet of Things: Survey and Taxonomy. 668-675. 10.1109/QRS-C55045.2021.00101.

[28] Ray, Partha & Dash, Dinesh & Kumar, Neeraj. (2020). Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. Computer Communications. 160. 10.1016/j.comcom.2020.05.029.

[29] Si-Ahmed, Ayoub & Al-Garadi, Mohammed & Boustia, Narhimene. (2022). Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things.

[30] Aceto, Giuseppe & Persico, Valerio & Pescapè, Antonio. (2018). The role of Information and Communication Technologies in Healthcare: Taxonomies, Perspectives, and Challenges. Journal of Network and Computer Applications. 107. 10.1016/j.jnca.2018.02.008.

[31] Sahshanu Razdan & Sachin Sharma (2021): Internet of Medical Things(IoMT): Overview, Emerging Technologies, and Case Studies, IETE Technical Review, DOI:10.1080/02564602.2021.1927863

[32] Rachida, Hireche & Mansouri, Houssem & Pathan, Al-Sakib. (2022). Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. Journal of Cybersecurity and Privacy. 2. 640-661. 10.3390/jcp2030033.

[33] H. Javdani, H. Kashanian, Internet of things in medical applications with a service-oriented and security approach: a survey. Health Technol. 8(1), 39–50 (2018)

[34] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, RFID technology for IoT-based personal healthcare in smart spaces. IEEE Internet Things J. 1(2), 144–152 (2014)

[35] GS1, EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface, GS1: Brussels, Belgium, (2015) pp. 1–152, https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf. Accessed 6 Sep. 2022

[36] L. M. Dang, M. J. Piran, D. Han, K. Min, H. Moon, A survey on internet of things and cloud computing for healthcare. Electronics 8(7), 768 (2019)

[37] Proceedings of the First ACM Conference on Wireless Network Security, WiSec'08, Alexandria, VA, USA, 31 March–2 April 2008; Association for Computing Machinery, New York, NY, USA (2008) pp. 140–147

[38] D. Z. Sun, J. D. Zhong, hash-based RFID security protocol for strong privacy protection. IEEE Trans. Consum. Electron. 58(4), 1246–1252 (2012)

[39] A. Alrawais, A. Alhothaily, C. Hu, X. Cheng, Fog computing for the Internet of Things: security and privacy issues. IEEE Internet Comput. **21**(2), 34–42 (2017)

[40] Cypress. PSoC® Creator Component Datasheet-Bluetooth Low Energy (BLE) 3.10,Description SIG adopted Profiles and Services Comprehensive APIs, (2015) pp. 408–943, https://www.cypress.com/file/232821/download. Acessed 6 Sep. 2021

[41] J. B. SIG, Bluetooth Specification, v. 3.0. EEE Spectr. (2009)

[42] A.M. Lonzetta, P. Cope, J. Campbell, B.J. Mohd, T. Hayajneh, Security vulnerabilities in Bluetooth technology as used in IoT. J. Sens. Actuator Netw. **7**(3), 28 (2018)

[43] S.R. Ramson, D.J. Moni, A case study on different wireless networking technologies for remote health care. Intell. Decis. Technol. **10**(4), 353–364 (2016)

[44] H. Fotouhi, A. Causevic, K. Lundqvist, M. Björkman, Communication and security in health monitoring systems–a review, in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. vol. 1 (IEEE, 2016), pp. 545–554

[45] X.Zhang, M.Wei, P.Wang, Y.Kim, Research and implementation of security mechanism in ISA100.11a networks, in *Proceedings of the 2009 9th*

International Conference on Electronic Measurement Instruments, Beijing, China, IEEE, 16–19 August 2009, pp. 4–716–4–721

[46] Y. Zeng, J. Cao, J. Hong, S. Zhang, L. Xie, Secure localization and location verification in wireless sensor networks: a survey. J. Supercomput. **64**, 685–701 (2013)

[47] Y. Wang, X. Ma, G. Leus, An UWB ranging-based localization strategy with internal attack immunity, in *Proceedings of the 2010 IEEE International Conference on Ultra-Wideband*, Nanjing, China, IEEE, 2(2010) pp. 1–4

[48] M. Flury, M. Poturalski, P. Papadimitratos, J.P. Hubaux, J.Y. Le Boudec, Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging, in *Proceedings of the 3rd ACM Conference on Wireless Network Security, WiSec'10*, Hoboken, NJ, USA, 22–24 March 2010, pp. 117–128

[49] M. Singh, P. Leu, S. Capkun, UWB with pulse reordering: securing ranging against relayand physical-layer attacks, in *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*, San Diego, CA, USA, 24–27 February 2019

[50] M. Sain, Y.J. Kang, H.J. Lee, Survey on security in Internet of Things: state of the art and challenges, in *Proceedings of the International Conference on Advanced Communication Technology, ICACT*, vol. 19–22 (IEEE, Bongpyeong, Korea, 2017), pp. 699–704

[51] T. Salman, R. Jain, A Survey of Protocols and Standards for Internet ofT hings, arXiv2019, arXiv:1903.1669

[52] G. Calcagnini, E. Mattei, F. Censi, M. Triventi, R. Lo Sterzo, E. Marchetta, P. Bartolini, Electromagnetic compatibility of WiFi technology with life-supporting medical devices, in *Proceedings of the World Congress on Medical Physics and Biomedical Engineering*, Munich, Germany, 7–12 September 2009 (Springer, Berlin/Heidelberg, Germany, 2009), pp. 616–619

[53] B.A. Mubdir, H.M.A. Bayram, Adopting MQTT for a multi protocols IoMT system. Int. J. Electr. Comput. Eng. *12*(1), 2088–8708 (2022)

[54] H. Peng, WIFI network information security analysis research, in *Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, IEEE, 21–23 April 2012, pp. 2243–2245

[55] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: a block architecture. IEEE Access **6**, 32700–32726 (2018)

[56] D.C. Yacchirema, C.E. Palau, M. Esteve, Enable IoT interoperability in ambient assisted living: active and healthy aging scenarios, in *Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 8–11 January 2017, pp. 53–58

[57] Zigbee Alliance Inc, ZigBee Specification, Zigbee Alliance Inc. (2015), pp. 1–378, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee- specification.pdf. Accessed on 6 Sep. 2022

[58] S.M. Rana,M.A., Halim, M.H. Kabir, Design and implementation of a security improvement framework of Zigbee network for intelligent monitoring in IoT platform. Appl. Sci. **8**(11), 2305 (2018)

[59] T. Zhong, C. Mengjin, Z. Peng, W. Hong, Real-time communication in WIA-PA industrial wireless networks, in *Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, China, 9–11 July 2010, Vol 2, pp. 600–605

[60] C.R. Su, J. Hajiyev, C.J. Fu, K.C. Kao, C.H. Chang, C.T. Chang, A novel framework for a remote patient monitoring (RPM) system with abnormality detection. Health Policy Technol. **8**(2), 157–170 (2019). https://doi.org/10.1016/j.hlpt.2019.05.008

[61] X. Wang, L. Cui, Z. Guo, Advanced technologies in ad hoc and sensor networks, in *Proceedings of the 7th China Conference on Wireless Sensor Networks*, vol. 295 (2014), pp. 288

[62] W.Liang, X.Zhang, Y.Xiao, F.Wang, P.Zeng, H.Yu, Survey and experiments of WIA-PA specification of industrial wireless network. Wirel. Commun. Mob. Comput. **11**(8), 1197–1212 (2011)

[63] H. Fotouhi, A. Cauševic, M. Vahabi, M. Björkman, Interoperability in heterogeneous low- power wireless networks for health monitoring systems, in *Proceedings of the 2016 IEEE International Conference on Communications Workshops (ICC)*, Kuala Lumpur, Malaysia, 23–27 May 2016, pp. 393–398

[64] J. Olsson, 6LoWPAN Demystified, Texas Instruments: Dallas, TX, USA, 13(2014), https://www.ti.com/lit/wp/swry013/swry013.pdf?ts=1645202797751&ref_u

rl=https%253A% 252F%252Fwww.google.com%252F. Accessed 6 Sep. 2022

[65] P. Chen, Yokogawa electric corporation, using ISA100.11a wireless technology to monitor pressure and temperature in a refinery (2011)

[66] J. Haxhibeqiri, E. DePoorter, I. Moerman, J. Hoebeke, A survey of LoRaWAN for IoT: from technology to application. Sensors **18**(11), 3995 (2018)

[67] A. Mdhaffar, T.Chaari, K. Larbi, M. Jmaiel, B. Freisleben, IoT-based health monitoring via LoRaWAN, in *Proceedings of the IEEE EUROCON 2017–17th International Conference on Smart Technologies*, Ohrid, Skopje, 6–8 July 2017, pp. 519–524

[68] A. Yegin, T. Kramp, P. Dufour, R. Gupta, R. Soss, O. Hersent, D. Hunt, N. Sornin, LoRaWAN protocol: specifications, security, and capabilities, in *LPWAN Technologies for IoT and M2M Applications*. ed. by B.S. Chaudhari, M. Zennaro (Academic Press, Cambridge, MA, USA, 2020), pp. 37–63

[69] C. Gündogan, P. Kietzmann, M. Lenders, H. Petersen, T.C. Schmidt, M. Wählisch, NDN, CoAP, and MQTT: a comparative measurement study in the IoT, in *Proceedings of the 5th ACM Conference on Information-Centric Networking* (2018), pp. 159–171

[70] A. Hussain, T. Ali, F. Althobiani, U. Draz, M. Irfan, S. Yasin, S. Shafiq, Z. Safdar, A. Glowacz, G. Nowakowski, M.S. Khan, S. Alqhtani, Security framework for IoT based real-time health applications. Electronics **10**(6), 719 (2021)

[71] S.N. Swamy, D. Jadhav, N. Kulkarni, Security threats in the application layerin IOT applications, in *Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 10–11 February 2017, pp. 477–480

[72] T. Dey, S. Jaiswal, S. Sunderkrishnan, N. Katre, Health Sense: a medical use case of Internet of Things and Blockchain, in *Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, India, 7–8 December 2017, pp. 486–491

[73] V. Karagiannis, P. Chatzimisios, F. Vazquez-gallego, J. Alonso-zarate, Sensus: smart water network, rans. IoT Cloud Comput. **3**, 1–10 (2016)

[74] J. Mohammed, C. Lung, A. Ocneanu, A. Thakral, C. Jones, and A. Adler. Internet of things: Remote patient monitoring using web services and cloud computing. In: 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), pages 256–263, 2014.

[75] Chamandeep Kaur. The cloud computing and internet of things (IoT). International Journal of Scientific Research in Science, Engineering and Technology, 7:19–22, 01 2020.

[76] Nabil Sultan. Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management, 34:177–184, 04 2014.

[77] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., Jin, Y. Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. *J. Hardw. Syst. Secur.* **2018**, *2*, 97–110.

[78] Maher, O., Sitnikova, E. A Trustworthy Learning Technique for Securing Industrial Internet of Things Systems. *J. Intell. Syst. Internet Things* **2021**, *5*, 33–48.

[79] Thilakarathne, N.N., Kagita, M.K., Gadekallu, D.T.R. The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study. *Int. J. Eng. Manag. Res.* **2020**, *10*, 145–159.

[80] Thilakarathne, N.N. Security and Privacy Issues in IoT Environment. *Int. J. Eng. Manag. Res.* **2020**, *10*, 26–29.

[81] Yasser, I., Khalil, A.T., Mohamed, M.A., Khalifa, F. A New Chaos-based Approach for Robust Image Encryption. *J. Cybersecur. Inf. Manag.* **2021**, *7*, 51–64.

[82] Armerding, T. Medical Devices at Risk: 5 Capabilities That Invite Danger. *CSO Online* 2017. Available online: https:// www.csoonline.com/article/3202081/security/medical-devices-at-risk-5-capabilities-that-invite-danger.html (accessed on 6 Sep 2022).

[83] El-hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A. A survey of internet of things (IoT) Authentication schemes. *Sensors* **2019**, *19*, 1141.

[84] Kang, J., Adibi, S. A review of security protocols in mHealth wireless body area networks (WBAN). In Proceedings of the Future Network Systems and Security: First International Conference, FNSS, Paris, France, 11–13 June

2015; Doss, R., Piramuthu, S., Zhou, W., Eds.; Springer: Cham, Switzerland, 2015; pp. 61–83.

[85] 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.

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

[87] 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.

[88] 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.

[89] 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.

[90] 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.

[91] 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.

[92] 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.

[93] P. Kumar and H.-J. Lee, “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey,” Sensors, vol. 12, no. 1, pp. 55–91, Dec. 2011.

[94] Nieles M, Dempsey K, Yan PV. NIST special publication 800-12 revision 1 - an introduction to information security. *NIST Special Publ*. 2017. https://doi.org/10.6028/NIST.SP.800-12r1.

[95] Tiloca M, Raza S. Security mechanisms and technologies for constrained IoT devices. *IoT A to Z Technol Appl*. London: John Wiley & Sons; 2018;221.

[96] Newsome James, Shi Elaine, Song Dawn, Perrig Adrian. The sybil attack in sensor networks: analysis & defenses. Paper presented at: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, IPSN 2004; 2004: 259-268.

[97] Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the Internet of Things. *IEEE Commun Surv Tutor*. 2019;21(2):1636-1675. https://doi.org/10.1109/COMST.2018.2874978.

[98] Borgohain Tuhin, Kumar Uday, Sanyal Sugata. *Survey of Security and Privacy Issues of Internet of Things*. 2015.

[99] Reziouk A, Laurent E, Demay JC. *Practical security overview of IEEE 802.15.4*. New York, NY: Institute of Electrical and Electronics Engineers Inc; 2016.

[100] Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the Internet of Things: security and privacy issues. *IEEE Internet Comput*. 2017;21(2):34-42. https://doi.org/10.1109/MIC.2017.37.

[101] Alsubaei F, Abuhussein A, Shiva S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*. Institute of Electrical and Electronics Engineers Inc; 2017:112-120.

[102] Mohammadi Shahriar, Jadidoleslamy Hossein. *A Comparison of Link Layer Attacks on Wireless Sensor Networks*. 2011.

[103] Halperin D, Heydt-Benjamin TS, Ransford B. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. *2008 IEEE Symposium on Security and Privacy*. IEEE; 2008:129-142.

[104] Wang M, Yan Z. Privacy-preserving authentication and key agreement protocols for d2d group communications. *IEEE Trans Ind Inform*. 2018;14(8):3637-3647. https://doi.org/10.1109/TII.2017.2778090.

[105] Hummen René, Ziegeldorf Jan H, Shafagh Hossein, Raza Shahid, Wehrle Klaus. Towards Viable Certificate-based Authentication for the Internet of Things. *ACM Workshop on Hot Topics on Wireless Network Security and Privacy, co-located with ACM WiSec*. 2013.

[106] Ni J, Zhang K, Lin X, Shen XS. Securing fog computing for internet of things applications: challenges and solutions. *IEEE Commun Surv Tutor*. 2018;20(1):601-628. https://doi.org/10.1109/COMST.2017.2762345.

[107] Zhang P, Zhou M, Fortino G. Security and trust issues in Fog computing: a survey. *Future Generat Comput Syst*. 2018;88:16-27. https://doi.org/10.1016/j.future.2018.05.008.

[108] Awad A, Khanapi M, Ghani A, Arunkumar N. *Enabling Technologies for Fog Computing in Healthcare IoT Systems*. Vol 90. Amsterdam: Elsevier; 2019:62-78.

[109] Manogaran G, Varatharajan R, Lopez D, Malarvizhi P, Sundarasekar R, Thota C. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generat Comput Syst*. 2018;82:375-387.

[110] Esfahani A, Mantas G, Matischek R, et al. A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE IoT J*. 2017;6(1):288-296.

[111] Katagi Masanobu, Moriai Shiho. *Lightweight Cryptography for the Internet of Things*. 2008;2008:7–10.

[112] Nist *Draft NISTIR 8114, Report on Lightweight Cryptography*. Maryland: National Institute of Standards and Technology; 2016.

[113] William S. Cryptography and network security, 4/E, stallings2006cryptography. 2006; Pearson Education India.

[114] Mantas G, Lymberopoulos D, Komninos N. PKI security in large-scale healthcare networks. *J Med Syst*. 2012;36(3):1107-1116.

[115] Deogirikar Jyoti, Vidhate Amarsinh. Security Attacks in IoT: A Survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*; 2017:32-37.

[116] Stojmenovic Ivan, Wen Sheng. The Fog computing paradigm: scenarios and security issues. Paper presented at: Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, FedCSIS 2014; vol 2, 2014:1-8.

[117] Lounis A, Hadjidj A, Bouabdallah A, Challal Y. Secure and Scalable Cloud-Based Architecture for e-Health Wireless Sensor Networks. *2012 21st*

International Conference on Computer Communications and Networks (ICCCN). IEEE; 2012:1-7.

[118] Lorincz Konrad, Malan David J., Fulford-Jones Thaddeus R.F., et al. *Sensor Networks for Emergency Response: Challenges and Opportunities*. Piscataway, NJ: IEEE; 2004.

[119] Mantas G, Stakhanova N, Gonzalez H, Jazi HH, Ghorbani AA. Application-layer denial of service attacks: taxonomy and survey. *Int J Inf Comput Sec*. 2015;7(2-4):216-239.

[120] Sciancalepore S, Oligeri G, Pietro R. Strength of crowd (SOC)–defeating a reactive jammer in IoT with decoy messages. *Sensors (Switzerland)*. Multidisciplinary Digital Publishing Institute; 2018;18(10):3492. https://doi.org/10.3390/s18103492.

[121] G. Mooney. (2018). *Is HIPAA Compliant With the GDPR?* [Online]. Available: https://blog.ipswitch.com/is-hipaa-compliant-with-the-gdpr (accessed on 6 Sep 2022)

[122] N. Sufyan, N. A. Saqib, and M. Zia, ‘‘Detection of jamming attacks in 802.11b wireless networks,’’ *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, p. 208, 2013.

[123] P. Kumar and H.-J. Lee, ‘‘Security issues in healthcare applications using wireless medical sensor networks: A survey,’’ *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[124] A. Kogetsu, S. Ogishima, and K. Kato, ‘‘Authentication of patients and participants in health information exchange and consent for medical research: A key step for privacy protection, respect for autonomy, and trustworthiness,’’ *Frontiers Genet.*, vol. 9, p. 167, Jun. 2018.

[125] P. Crilly and V. Muthukkumarasamy, ‘‘Using smart phones and body sensors to deliver pervasive mobile personal healthcare,’’ in *Proc. 6th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process.*, Dec. 2010, pp. 291–296.

[126] Sabyasachi Chakraborty, Satyabrata Aich, and Hee-Cheol Kim. A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Com- munication Technology (ICACT)*, pages 260–264. IEEE, 2019.

[127] Pejman Niksaz and Mashhad Branch. Wireless body area networks: attacks and countermeasures. *Int. J. Sci. Eng. Res*, 6(9):556–568, 2015.

[128] A. Evesti, T. Kanstrén and T. Frantti, "Cybersecurity situational awareness taxonomy," *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2017, pp. 1-8, doi: 10.1109/CyberSA.2017.8073386.

[129] H. Hindy *et al*., "A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems," in *IEEE Access*, vol. 8, pp. 104650-104675, 2020, doi: 10.1109/ACCESS.2020.3000179.

[130] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103-2115, April 2019, doi: 10.1109/JIOT.2018.2869847.

[131] A. Phadke and S. Ustymenko, "Updating the Taxonomy of Intrusion Detection Systems," *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2021, pp. 1085-1091, doi: 10.1109/COMPSAC51774.2021.00148.

[132] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, pp. 91-98, doi: 10.1109/EISIC.2017.20.

[133] Bromander, Siri, Audun Jøsang and Martin Eian. "Semantic Cyberthreat Modelling." *STIDS* (2016).

[134] Ahmed, Monjur & Litchfield, Alan. (2017). Taxonomy for Identification of Security Issues in Cloud Computing Environments. Journal of Computer Information Systems. 58. 79-88. 10.1080/08874417.2016.1192520.

[135] Mayzaud, Anthéa & Badonnel, Rémi & Chrisment, I. (2016). A Taxonomy of Attacks in RPL-based Internet of Things. 18.

[136] I. Butun, S. D. Morgera and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 266-282, First Quarter 2014, doi: 10.1109/SURV.2013.050113.00191.

[137] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *NIST special publication*, *800*(150).

[138] ENISA Report: A good practice guide of using taxonomies in incident prevention and detection (Dec 2016)

https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-preventiondetection/at_download/fullReport (accessed on 6 Sep 2022).

[139] ENISA Report: Information sharing and common taxonomies between CSIRTs and Law Enforcement (Dec 2015) https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomiesbetween-csirts-and-law-enforcement/ (accessed on 6 Sep 2022).

[140] R. Derbyshire, B. Green, D. Prince, A. Mauthe and D. Hutchison, "An Analysis of Cyber Security Attack Taxonomies," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 153-161, doi: 10.1109/EuroSPW.2018.00028.

[141] C. Easttom and W. Butler, "A Modified McCumber Cube as a Basis for a Taxonomy of Cyber Attacks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0943-0949, doi: 10.1109/CCWC.2019.8666559.

[142] S. G. Abbas, F. Hashmat and G. A. Shah, "A Multi-layer Industrial-IoT Attack Taxonomy: Layers, Dimensions, Techniques and Application," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1820-1825, doi: 10.1109/TrustCom50675.2020.00249.

[143] N. A. Noureldien, "A novel taxonomy of MANET attacks," 2015 International Conference on Electrical and Information Technologies (ICEIT), 2015, pp. 109-113, doi: 10.1109/EITech.2015.7162947.

[144] Hansman, Simon & Hunt, Ray. (2005). A taxonomy of network and computer attacks. Computers & Security. 24. 31-43. 10.1016/j.cose.2004.06.011.

[145] Zhao, Zhongwen & Dai, Yingchun. (2012). A New Method of Vulnerability Taxonomy Based on Information Security Attributes. 739-741. 10.1109/CIT.2012.152.

[146] A. Romanenko, M. Tanjimuddin, P. Raussi, M. Aro, V. Tikka and S. Honkapuro, "Taxonomy of Security Threats in Energy Systems," 2020 17th International Conference on the European Energy Market (EEM), 2020, pp. 1-7, doi: 10.1109/EEM49802.2020.9221940.

[147] Chapman, Ian & Leblanc, Sylvain & Partington, Andrew. (2011). Taxonomy of cyber attacks and simulation of their effects.. 73-80.

[148] J. Wei and J. Wei, "Survey of network and computer attack taxonomy," 2012 IEEE Symposium on Robotics and Applications (ISRA), 2012, pp. 294-297, doi: 10.1109/ISRA.2012.6219182.

[149] Boyanov, P. K. (2013). A taxonomy of the cyber attacks. *SCIENTIFIC AND APPLIED RESEARCH*, *3*(20), 3.

[150] Dorsemaine, B., Gaulier, J. P., Wary, J. P., Kheir, N., & Urien, P. (2015, September). Internet of things: a definition & taxonomy. In *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies* (pp. 72-77). IEEE.

[151] Babič, M., & Jerman-Blažič, B. (2016, May). New cybercrime taxonomy of visualization of data mining process. In *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 349-351). IEEE.

[152] Ahmad, N. H., & Aljunid, S. A. (2011, December). Understanding vulnerabilities by refining taxonomy. In *2011 7th International Conference on Information Assurance and Security (IAS)* (pp. 25-29). IEEE.

[153] Polash, F., Abuhussein, A., & Shiva, S. (2014, December). A survey of cloud computing taxonomies: Rationale and overview. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 459-465). IEEE.

[154] Joshi, C., Singh, U. K., & Tarey, K. (2015). A review on taxonomies of attacks and vulnerability in computer and network system. *International Journal*, *5*(1).

[155] Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010, July). Proposed security model and threat taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications* (pp. 420-429). Springer, Berlin, Heidelberg.

[156] Al-Kahla, W., Shatnawi, A. S., & Taqieddin, E. (2021, May). A Taxonomy of Web Security Vulnerabilities. In *2021 12th International Conference on Information and Communication Systems (ICICS)* (pp. 424-429). IEEE.

[157] Lackner, Maximilian & E, Markl & A, Mohamed. (2018). Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities. Journal of Information Technology & Software Engineering. 08. 10.4172/2165-7866.1000250.

[158] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[159] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *Proc. IEEE Int. Conf. Privacy Security Mobile Syst.*, May 2014, pp. 1–8, doi: 10.1109/PRISMS.2014.6970594.

[160] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks", *Springer J. Wireless Network Security*, pages 159-180, 2007.

[161] T. Casey , "Threat Agent Library Helps Identify Information Security Risks," *Intel White Paper, September*, 2007.

[162] T. Casey, "Understanding cyber threat motivations to improve defense," *Intel White Paper*, 2015.

[163] MITRE,"Common Vulnerabilities and Exposures," https://cve.mitre.org.

[164] NIST, "National Vulnerability Database," https://nvd.nist.gov/.

[165] Mitre, "Common Platform Enumeration," https://cpe.mitre.org/specification/.

[166] MITRE, "Common Weakness Enumeration," https://cwe.mitre.org.

[167] MITRE, "Common Attack Pattern Enumeration and Classification," https://capec.mitre.org/.

[168] MITRE, "Adversarial Tactics, Techniques and Common Knowledge," https://attack.mitre.org/.

[169] F. Kolini & L. Janczewski, "Cyber Defense Capability Model: A Foundation Taxonomy." *In CONF-IRM,* pp. 32, 2015.

[170] D. Papp, Z. Ma, & L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy." *In the 13th Annual Conference on Privacy, Security and Trust (PST)*, pp. 145-152, 2015.

[171] N. Abrek, "Attack Taxonomies and Ontologies." In *Seminar Future Internet SS2014, Network Architectures and Services*, 2015.

[172] C. Joshi & U. Singh, "Admit-A five dimensional approach towards standardization of network and computer attack taxonomies." *International Journal of Computer Applications*, vol. 100, no. 5, 2014.

[173] Kjaerland, M., "A taxonomy and comparison of computer securityincidents from the commercial and government sectors". Computers and Security, 25:522–538, October 2005.

[174] Carlson, J. (2017). Unidimensional Vertical Scaling in Multidimensional Space. ETS Research Report Series, 2017(1), pp.1-28

[175] Levy, S. (2014). Facet Theory. Encyclopedia of Quality of Life and Well-Being Research, pp.2112-2119.

[176] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[177] Hansman, S., Hunt R., "A taxonomy of network and computer attacks". Computer and Security (2005).

[178] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[179] Mirkovic, J., and Reiher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In ACM CCR (April 2004)

[180] Lough, Daniel. "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[181] I. Ghafir and V. Prenosil, "Advanced Persistent Threat and Spear Phishing Emails." International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[182] Rodrigues JJPC, Rezende SDB, Junqueira HA, et al. Enabling technologies for the internet of health things. *IEEE Access*. 2018;6:13129-13141. https://doi.org/10.1109/ACCESS.2017.2789329.

[183] Moosavi SR, Gia TN, Nigussie E, et al. End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generat Comput Syst*. 2016;64:108-124. https://doi.org/10.1016/j.future.2016.02.020.

[184] Esfahani A, Mantas G, Silva H, Rodriguez J, Neves JC. An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems. *EURASIP J Wirel Commun Netw*. 2016;2016(1):113.

[185] Esfahani A, Mantas G, Yang D, Nascimento A, Rodriguez J, Neves J. *Towards Secure Network Coding-Enabled Wireless Sensor Networks in Cyber-Physical Systems*. Boca Raton, FL: CRC Press; 2015:395-414.

[186] Fengou M-A, Mantas G, Lymberopoulos D, Komninos N, Fengos S, Lazarou N. A new framework architecture for next generation e-health services. *IEEE J Biomed Health Inform*. 2012;17(1):9-18.

[187] Islam S, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: a comprehensive survey. *IEEE Access*. 2015;3:678-708. https://doi.org/10.1109/ACCESS.2015.2437951.

[188] Hommersom A, Lucas PJF, Velikova M, et al. *Moshca-My Mobile and Smart Health Care Assistant*. Piscataway, NJ: IEEE; 2013:188-192.

[189] L. D. X. Shancang Li and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, pp. 243–259, 2015.

[190] L. P. Luca Mainetti and A. Vilei, "Evolution of wireless sensor networks towards the internet of things: a survey," in *Proc. Software, Telecommunications and Computer Networks (SoftCOM), 2011*, Dubrovnik, Croatia, 2011, pp. 1–6.

[191] A. Avizienis, J-C. Laprie, B. Randell, and C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE Trans. De- pendable Secur. Comput., vol. 1, no. 1, pp. 1133, 2004.

[192] R. von Solms and J. van Niekerk, From Information Security to Cyber Security, Computers & Security, pp. 97102, 2013.

[193] Yaacoub JPA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2020) Securing internet of medical things systems: limitations, issues and recommendations. Future Gener Comput Syst 105:581–606

[194] Alsubaei F, Abuhussein A, Shiva S (2017) Security and privacy in the internet of medical things: taxonomy and risk assessment. In: 2017 IEEE 42nd conference on local computer networks work- shops (LCN workshops). IEEE, pp 112–120

[195] Leite C, Gondim JJ, Barreto PS, Caetano MF, Alchieri EA (2019) Pentest on internet of things devices. In: 2019 XLV Latin American computing conference (CLEI). IEEE, pp 1–10

[196] Khan RU, Zhang X, Alazab M, Kumar R (2019) An improved convolutional neural network model for intrusion detection in networks. In: 2019 cybersecurity and cyberforensics conference ing (CCC). IEEE, pp 74–77

[197] Alazab M, Broadhurst R (2016) Spam and criminal activity. Trends Issues Crime Crim Justice 526:1–20

[198] Javed AR, Ahmed W, Alazab M, Jalil Z, Kifayat K, Gadekallu TR (2022) A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. IEEE Access

[199] Nagarajan G, Babu LD (2022) Missing data imputation on biomedical data using deeply learned clustering and l2 regularized regression based on symmetric uncertainty. Artif Intell Med 123:102214

[200] Nagarajan G, Dhinesh Babu L (2021) A hybrid feature selection model based on improved squirrel search algorithm and rank aggregation using fuzzy techniques for biomedical data classification. Netw Model Anal Health Inform Bioinform 10(1):1–29

[201] *WHO Coronavirus (COVID-19) Dashboard*. (n.d.). With Vaccination Data. Retrieved September 25, 2022, from https://covid19.who.int/

[202] Jacobsson, A., Boldt, M., Carlsson, B. A risk analysis of a smart home automation system. Future Gener. Comput. Syst. 2016, 56, 719–733

[203] Alsubaei, F., Abuhussein, A., Shiva, S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9–12 October 2017; pp. 112–120.

[204] Darwish, S., Nouretdinov, I., Wolthusen, S.D. Towards composable threat assessment for medical IoT (MIoT). Procedia Comput. Sci. 2017, 113, 627–632.

[205] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A. Secure medical data transmis- sion model for IoT-based healthcare systems. IEEE Access 2018, 6, 20596–20608.

[206] Tarouco, L.M.R., Bertholdo, L.M., Granville, L.Z., Arbiza, L.M.R., Carbone, F., Marotta, M., De Santanna, J.J.C. Internet of Things in healthcare: Interoperatibility and security issues. In Proceedings of the 2012 IEEE

International Conference on Communications (ICC), Ottawa, ON, USA; 2012; pp. 6121–6125.

[207] Hossain, M., Islam, S.R., Ali, F., Kwak, K.S., Hasan, R. An internet of things-based health prescription assistant and its security system design. Future Gener. Comput. Syst. 2018, 82, 422–439

[208] Pirbhulal, S., Samuel, O.W., Wu, W., Sangaiah, A.K., Li, G. A joint resource-aware and medical data security framework for wearable healthcare systems. Future Gener. Comput. Syst. 2019, 95, 382–391.

[209] Sebestyen, G., Hangan, A., Oniga, S., Gál, Z. eHealth solutions in the context of Internet of Things. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–6.

[210] Kumari, A., Tanwar, S., Tyagi, S., Kumar, N. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. Comput. Electr. Eng. 2018, 72, 1–13.

[211] Silva, C.A., Aquino, G.S., Melo, S.R., Egídio, D.J. A fog computing-based architecture for medical records management. Wirel. Commun. Mob. Comput. 2019, 2019, 1968960.

[212] Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Andreescu, S. Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In Proceedings of the 2015 IEEE International Conference on Services Computing, New York City, NY, USA, 27 June–2 July 2015; pp. 285–292.

[213] Elsharkawy, M., Al Masri, A.N. A Novel Image Encryption with Deep Learning Model for Secure Content based Image Retrieval. J. Cybersecur. Inf. Manag. 2019, 0, 54–64.

[214] Zhao, W., Wang, C.,Nakahira, Y. Medical Application on Internet of Things. In Proceedings of the IET International Conference on Communication Technology and Application (ICCTA 2011), Beijing, China, 14–16 October 2011.

[215] Dimitrov, D.V. Medical internet of things and big data in healthcare. Healthc. Inform. Res. 2016, 22, 156–163.

[216] Hu, F., Xie, D., Shen, S. On the application of the internet of things in the field of medical and health care. In Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and

IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 2053–2058.

[217] Gómez, J., Oviedo, B., Zhuma, E. Patient monitoring system based on internet of things. Procedia Comput. Sci. 2016, 83, 90–97.

[218] Sangpetch, O., Sangpetch, A. Security context framework for distributed healthcare iot platform. In Proceedings of the Internet of Things Technologies for HealthCare, Västerås, Sweden, 18–19 October 2016; Springer: Cham, Switzerland, 2016; pp. 71–76.

[219] Rghioui, A., L'aarje, A., Elouaai, F., Bouhorma, M. The internet of things for healthcare monitoring: Security review and proposed solution. In Proceedings of the 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), Tetouan, Morocco, 20–22 October 2014; pp. 384–389.

[220] Laplante, P.A., Laplante, N. The internet of things in healthcare: Potential applications and challenges. It Prof. 2016, 18, 2–4.

[221] Li, C., Hu, X., Zhang, L. The IoT-based heart disease monitoring system for pervasive healthcare service. Procedia Comput. Sci. 2017, 112, 2328–2334.