Cyber-Attacks Classification in the Internet of Medical Things

Issam Najah   
Laboratoire Smart Information and Communication Technologies (SmartICT)-- Smart Systems & Cybersecurity Team  
ENSA of Oujda , Université Mohamed Premier, Morocco  
issam.najah@ump.ac.ma

line 1: 2nd Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 3rd Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

*Abstract*—The recent advances in information technology have ushered in a new era known as the Internet of Things (IoT). This technology enables objects (things) to connect to the Internet and share data, facilitating information transfer and reception between two or more linked devices over the internet. Specifically, the modern advancements in the IoT have given rise to the Internet of Medical Things (IoMT), which is increasingly significant in healthcare. IoMT plays a crucial role in establishing a safer and more efficient healthcare system, reducing healthcare costs, providing timely medical assistance, and enhancing the standard of medical care. However, the proliferation of IoMT devices poses various safety issues, making it challenging to ensure a high level of security and confidentiality.

Therefore, security has emerged as one of the primary challenges to address. This study comprehensively analyzes the security-related difficulties and potential threat sources in the IoMT. After discussing the security challenges, we propose a new classification of attacks in IoMT based on different criteria. This classification aids researchers in understanding and addressing each attack, leading to the development of robust attack detection mechanisms.

Keywords— IoMT, healthcare, attacks, taxonomy, classification, Security

# Introduction

The concept of the Internet of Things (IoT) has garnered significant attention in the modern world due to its revolutionary impact on human life. It offers a wide range of user-friendly solutions, making human life more convenient and automating interactions between humans and their environment. IoT finds applications in various fields such as smart grids, smart homes, smart retail, smart agriculture, smart cities, and more. The deployment of IoT has increased substantially in communities worldwide. As of 2022, the number of linked IoT devices had reached 43 billion, and it is projected to reach about 125 billion by 2030, driven by market demand [1].

The term "IoT-based Healthcare" or "Internet of Medical Things (IoMT)" refers to a collection of internet-connected devices used to carry out tasks and provide services that support healthcare. IoMT leverages small wearable devices or implantable sensors to gather patients' essential bodily data and track their pathological information, making it a new technology for e-healthcare. The IoMT has shown great promise in improving health assurance and supports applications like wireless body area networks and implantable medical devices (WBAN) [2]. However, the increasing complexity of IoMT infrastructures, driven by numerous devices using different services, technologies, and protocols, has led to vulnerabilities in the system.

Due to a large number of IoMT devices and the rapid development of new components Presently, there are security and data protection issues in IoMT due to the large number of devices and rapid market developments. IoMT is particularly susceptible to attacks since there are no specific security standards listing its vulnerabilities and weaknesses.

Before implementing security measures to safeguard IoMT, it is essential to understand the types of attacks and vulnerabilities it faces, including the attack mechanisms, purposes, and consequences. Collecting information about these attacks and threats enables the classification of attacks, facilitating subsequent steps. For each class of attacks, suitable intrusion detection and prevention methods and security mechanisms can be implemented. In this paper, the authors propose a new detailed attack classification in IoMT based on different criteria, such as IoMT level security, concepts, impact, and behaviors. This classification will help present effective security solutions to tackle these attacks.

The paper's organization is as follows: Section 2 focuses on the five-layer IoMT architecture. Section 3 provides an overview of some previous research. Section 4 summarizes the most famous IoMT attacks. Section 5 presents the authors' new classifications of attacks in IoMT. Finally, the paper concludes..

# Related Work

According to the literature research, it is evident that the focus on classification attacks in the context of IOMT (Internet of Medical Things) is relatively limited when compared to traditional IoT. Nevertheless, due to the increasing significance of IOMT in the healthcare sector, there has been a noticeable emergence of studies that concentrate on identifying and mitigating classification attacks specifically targeted at medical IoT systems. Below, I will highlight some related works on classification attacks in IOMT:

in [3] 2017, F. Alsubaei, A. Abuhussein, and S. Shiva discussed a taxonomy of security and privacy issues specific to IoMT. Their proposed taxonomy highlights security and privacy concerns based on their appearance in the five-layered IoT model and outlines the properties of these issues. They also introduced a risk assessment approach based on the taxonomy to consider new or unknown threats and features.

in [4] 2017, S. Bhuyan et al ddressed major privacy and security concerns in mobile health and identified relevant open problems while providing future research directions for electronic health services.

in [5] 2018, according to A. Djenna and D. Eddine Saidouni, discussed IoMT technology's three layers (perception, network, and application layers) and classified attacks occurring in each layer. They also described various threats, such as malicious actions, system and network failures, human errors, and natural phenomena, that can significantly impact a health system.

The authors Dr. Y. Perwej, N. Akhtar, N. Kulshrestha, and P. Mishra of [6] 2022 examined the main privacy and security concerns related to mobile health and highlighted significant open problems and future research directions for electronic health services.

Based on our observations, prior research has primarily focused on classifying IoMT (Internet of Medical Things) attacks. However, none of the studies have comprehensively addressed security attacks from various other important criteria. While many articles describe security attacks within each layer of the IoMT architecture, there remains a significant gap in providing a holistic analysis that covers multiple dimensions of IoMT security.

Therefore, this study aims to address this gap by proposing a new, detailed attack classification in IoMT based on different criteria, including IoMT level security, concepts, impact, behaviors, and more. By doing so, the research seeks to offer researchers a more comprehensive perspective on the security challenges and potential threats within the IoMT landscape.

The comprehensive approach taken in this study is anticipated to be immensely helpful for researchers seeking to gain a deeper understanding of the complexities of IoMT security. Moreover, it is expected to contribute significantly to the development of more effective defense mechanisms to safeguard IoMT systems against a wide array of security threats. Ultimately, this research aims to enhance the overall security posture of IoMT deployments and foster safer and more reliable medical IoT technologies in the future.

# Our Classification

The majority of IoMT objects and apps, sadly, are neither managed nor built to stop intrusions, which surely increases the surface area and cyber-attack vectors that are directed at this kind of infrastructure. In this section, we classify attacks related to the IoMT based on different criteria.

Security issues are divided into many categories, such as attacks based on targets, impact, encryption, application layer protocol, security concepts, and communication technology.

However, it is essential to note that the lack of standardized security measures in IoMT devices and applications exposes them to potential vulnerabilities and makes them attractive targets for cyber attackers. By classifying attacks based on various criteria, we can gain a more comprehensive understanding of the threats IoMT systems face and develop targeted and robust security measures to protect sensitive medical data and ensure the safety and privacy of patients [7].

Through this classification approach, researchers and stakeholders can effectively assess the risks associated with IoMT deployments and implement proactive security measures to mitigate potential attacks. Furthermore, a better understanding of the different attack vectors will enable the development of secure IoMT architectures and protocols, ultimately improving the overall cybersecurity posture of healthcare systems and promoting trust in the adoption of IoMT technologies.

## Classification Based on Layers

The IoMT (Internet of Medical Things) structure typically consists of five layers: Perception Layer, Network Layer, Middleware Layer, Application Layer, and Business Layer.

Each layer in the IoMT architecture plays a crucial role in the functionality and security of the system:.

* Perception Layer: This is the lowest layer and involves the physical devices and sensors that collect data from the environment or patients. These devices may include wearable health trackers, medical sensors, and monitoring equipment.
* Network Layer: The network layer facilitates the communication between the devices and the central infrastructure. It involves various communication technologies, such as Wi-Fi, Bluetooth, Zigbee, or cellular networks, to transmit the collected data securely and efficient [8].
* Middleware Layer: The middleware layer acts as an intermediary between the lower-level IoT devices and the upper-level applications. It manages data processing, storage, and routing, and may also handle security protocols and data integration [9].
* Application Layer: The application layer is where the data from the IoT devices is processed, analyzed, and transformed into valuable insights. It includes various healthcare applications and platforms that enable medical professionals to monitor and manage patient data, as well as provide personalized healthcare services [3].
* Business Layer: The business layer focuses on the overall management and governance of the IoMT system. It involves decision-making processes, business intelligence, and strategic planning to ensure the effective and secure deployment of IoMT solutions in healthcare organizations [3].

In order to guarantee the highest level of reliability, The medical devices connected via the Internet must be managed in a diverse way due to the sensitivity of medical systems. Consequently, a flexible layered architecture is required.

A layered architecture, with each layer providing specific functionality, is presented by the IoMT five-layer model the above-mentioned. Different security attacks exist for each functionality. As a result, we categorize security attacks and privacy problems as they arise in each layer as shown in Fig.1.

## Classification based on Security Concepts

This categorizes IoMT attacks based on Security Concepts. The Security Concepts-based classification is important as it highlights the fundamental security goals in developing measures for IoMT systems:

* Confidentiality: Confidentiality is jeopardized when someone gains unauthorized access to sensitive data. Healthcare data often contain private and personal making the preservation of confidentiality crucial
* Availability: Availability ensures that information is accessible to authorized individuals when needed. It provides assurance that authorized users will always be able to access the IoMT system and its data.
* Integrity: Data integrity is essential in healthcare since it reflects diagnoses, treatments, or patients' health status. Unauthorized alterations to data could result in inaccurate diagnoses and cause irreparable harm.
* Authentication: Device authentication is the first step in ensuring a secure data transmission session. It involves identifying devices and approving the actions they can perform within the network. Authentication guarantees that only legitimate devices accept and execute authorized requests. It encompasses both authorization and identification.
* Non-repudiation: Non-repudiation prevents individuals from denying or rejecting the occurrence of an event, transaction, or activity. This ensures that actions or communications conducted within the IoMT system can be verified and traced back to the responsible parties.

Fig.2 categorize security attacks and privacy problems based on Security Concepts.

By categorizing IoMT attacks based on these security concepts, researchers and stakeholders can develop targeted security measures to address specific vulnerabilities and protect IoMT systems from various types of security breaches. Understanding these security goals is crucial for building robust and secure IoMT architectures that maintain patient privacy, data integrity, and system availability while mitigating potential risks posed by cyber-attacks and unauthorized access.

## Classification based on Impact

We can introduce a new classification scheme that categorizes attacks into three subclasses based on their impact: "Low," "Medium," and "High." This classification aims to assess the severity and consequences of each attack [10].

* Low Impact Attacks: These attacks have minimal or limited adverse effects on IoMT systems and patient data. They may cause minor disruptions or inconvenience but do not significantly compromise the confidentiality, integrity, or availability of critical medical information.
* Medium Impact Attacks: Attacks falling into this category have a moderate level of impact on IoMT systems. They may lead to partial system unavailability, temporary data loss, or breaches in data confidentiality, potentially affecting patient care and requiring remediation efforts.
* High Impact Attacks: High impact attacks are the most severe and pose significant threats to IoMT systems and patient safety. They can cause extended system outages, substantial data breaches, manipulation of medical records, or disruption of critical healthcare services, leading to severe consequences for patients and healthcare providers.

Fig.3 categorize security attacks and privacy problems based on impact.

By classifying attacks into these three subclasses, security professionals and stakeholders can prioritize their response and allocate appropriate resources to address the most critical threats. It helps healthcare organizations better understand the potential risks posed by different attacks and develop proactive defense mechanisms to safeguard sensitive patient data and ensure the reliable functioning of IoMT systems. Additionally, this classification framework can aid in risk assessments and decision-making processes when designing security strategies and policies for IoMT deployments.

## Classification based on Encryption

This kind of attacks aims to break the encryption system. in [7], they classify this class into two subclasses:

* Cryptanalysis Attack: Its goal is to recover the encryption key needed to disable the IoMT system's encryption feature.
* Side channel Attack: Attackers can use strategies like electromagnetic and power analysis to discover the encryption key to access compromised data.

Fig.4 categorize security attacks and privacy problems based on Encryption.

Both cryptanalysis and side-channel attacks are serious threats to the security of IoMT systems. The attackers' ability to break the encryption can lead to significant breaches in data confidentiality, posing risks to patient privacy and medical information. To mitigate these attacks, IoMT systems must employ robust encryption techniques, regularly update encryption keys, and implement additional security measures to protect against cryptanalysis and side-channel vulnerabilities. By understanding the nature of these attacks and their potential impact, researchers and security professionals can design more effective and resilient encryption solutions to safeguard IoMT data and maintain the integrity of medical information.

## Classification based on Communication Technologies

A new classification of attacks using communication technologies is presented in this section and is based on two categories [7]:

* Short-range: RFID, NFC, WSN, 6LowPan, Z-Wave, Zigbee, Bluetooth, Wi-Fi, BLE, LR-WPANs,IEEE 802.11 ah, IEEE 802.15.4.
* Long-range: Sigfox, LoRa/LoRaWAN, NB-IoT, Satellite, LTE/LTE-A, 3G/4G, GSM, GPRS, GPS.

Fig.5 categorize security attacks and privacy problems based on Communication Technologies .

This classification helps in understanding the specific attack vectors based on short-range and long-range communication technologies in IoMT systems. By identifying and addressing these threats, healthcare organizations can implement appropriate security measures, such as encryption, authentication protocols, and intrusion detection, to protect IoMT communication channels and ensure the privacy and integrity of patient data. It is crucial to develop robust security strategies that account for the unique challenges posed by both short-range and long-range communication technologies to create a secure and resilient IoMT infrastructure. Ongoing monitoring and proactive response to potential attacks are essential for maintaining a reliable and secure IoMT ecosystem.

## Classification based on Behavior

Attacks in IoMT are grouped based on behavior, providing valuable insights for proactive security preparations and aiding in understanding the motives and objectives of the attacks. The classifications are as follows:

* Passive Attacks: Passive attacks involve listening or monitoring network communications without altering the data or the functioning of the network. These attacks are usually stealthy and aim to gather sensitive information covertly.
* Active Attacks: Active attacks take the data acquired from passive attacks and actively compromise the IoMT system. Unlike passive attacks, active attacks involve manipulation or alteration of data or network operations

Fig.6 categorize security attacks and privacy problems based on Communication Technologies.

By categorizing attacks into passive and active categories, security professionals can better understand the varying behaviors and techniques used by adversaries. This knowledge is crucial for designing effective security strategies that can detect and mitigate attacks proactively, protecting the confidentiality, integrity, and availability of IoMT systems and patient data. Additionally, understanding the motives and objectives behind passive and active attacks helps healthcare organizations identify potential weaknesses and strengthen their IoMT infrastructure to defend against emerging threats effectively. Continuous monitoring and timely response are essential components of a robust security approach to ensure the reliability and safety of IoMT deployments.

## Classification based on Source

Attacks in IoMT can be categorized based on their source, which aids in attributing the attacker and understanding the attack's origin. The classifications are as follows:

* Local (Internal): Local attacks require the attacker's proximity to the compromised system or their physical presence on-site. In such attacks, the intruder is physically close to a medical device or the IoMT infrastructure [3].
* Remote (External) : Remote attacks involve exploiting system flaws, vulnerabilities, or using malware to compromise the IoMT infrastructure without the attacker physically being close to the victim device [3].

Fig.4 categorize security attacks and privacy problems based on source.

Understanding the source of the attack is essential for attribution, incident response, and implementing targeted security measures. By classifying attacks into local and remote categories, healthcare organizations can focus on the specific risks associated with each type and develop appropriate security strategies to mitigate such threats effectively. This comprehensive approach ensures the security and reliability of IoMT systems, protecting patient data, and minimizing the risk of unauthorized access or malicious activities in healthcare environments.

## Classification based on Target

Targets in IoMT attacks can be classified into three main categories: User, Hardware, and System/Application. Each category involves different types of attacks with specific objectives. The classifications are as follows:

* User: causing the user physical harm, such turning off medical life support systems.
* Hardware: This covers any physical hardware loss, physical alteration, or attacks involving IoMT device [3].
* System/application : This involves changing the IoMT application or a system-level application to make it impossible to use the system [3].

Fig. 8 categorize security attacks and privacy problems based on target.

Understanding the target of the attack is crucial for determining the attacker's motives and the potential consequences of the attack. By categorizing attacks into user, hardware, and system/application targets, healthcare organizations can develop targeted security measures to protect patients, safeguard IoMT devices, and ensure the overall integrity and availability of healthcare services. Moreover, this knowledge aids in identifying potential vulnerabilities and implementing appropriate security protocols to defend against various attack vectors effectively. Ongoing monitoring and incident response readiness are essential to maintaining a secure and resilient IoMT ecosystem.

## Classification based on application layer Protocols

There are many application protocols that can be found in the literature, such as the Constrained Application Protocol (CoAP), the Message Queue Telemetry Transport (MQTT), and the Extensible Message and Presence Protocol (XMPP), each protocol has its attacks.

Fig.9 categorize security attacks and privacy problems based on application layer Protocols.

It's important to note that these are just a few examples, and each application protocol may have additional attack vectors. As IoMT systems rely on diverse application protocols for communication, it is crucial to assess the security risks associated with each protocol and implement appropriate security measures to safeguard against potential attacks. Regular security audits, timely patching of vulnerabilities, and strong authentication mechanisms are essential to maintain the integrity and security of IoMT communications using these application protocols.

# Conclusion

The increasing prevalence of serious security risks and malicious actions targeting IoMT devices has become a significant concern in the development of IoMT. These cyberattacks not only result in substantial financial losses but can also lead to human casualties, making the protection of user privacy a critical challenge in the IoMT landscape.

To design effective security solutions, it is imperative to gain a comprehensive understanding of the security issues surrounding IoMT. This document aims to identify and recognize the various cyberattacks related to IoMT devices, leading to the presentation of a new classification of cyberattacks specific to IoMT infrastructure. While achieving full security for IoMT devices may take time, comprehending the different cyberattacks is a crucial first step in developing robust defenses.

The proposed classification of cyberattacks in IoMT is based on various criteria such as the target, source, and behavior of the attacks. By categorizing attacks according to these factors, researchers and security professionals can gain deeper insights into the unique characteristics and motives behind each attack type. This understanding paves the way for the development of targeted and effective security solutions tailored to counteract specific cyberattack vectors.

With this classification as a foundation, efforts are underway to create security solutions that protect IoMT devices and the sensitive data they handle. These solutions will focus on mitigating the vulnerabilities identified through the classification, strengthening the security posture of IoMT systems, and safeguarding user privacy and patient safety.

While achieving full IoMT security is an ongoing and challenging process, the commitment to understanding cyberattacks and developing effective defenses is crucial for ensuring the trustworthy and safe adoption of IoMT technologies. Through continuous research, collaboration, and innovation, the IoMT community can work together to build a secure and resilient IoMT ecosystem that benefits patients, healthcare providers, and society as a whole.

##### References

[1] ‘IoT : nombre d’appareils connectés dans le monde 2015-2025’, *Statista*. https://fr.statista.com/statistiques/584481/internet-des-objets-nombre-d-appareils-connectes-dans-le-monde-2020/ (accessed Jun. 23, 2023).

[2] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, ‘Security and Privacy in the Medical Internet of Things: A Review’, *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, 2018, doi: 10.1155/2018/5978636.

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

[4] S. S. Bhuyan *et al.*, ‘Privacy and security issues in mobile health: Current research and future directions’, *Health Policy Technol.*, vol. 6, no. 2, pp. 188–191, Jun. 2017, doi: 10.1016/j.hlpt.2017.01.004.

[5] A. Djenna and D. Eddine Saidouni, ‘Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure’, in *2018 2nd Cyber Security in Networking Conference (CSNet)*, Paris: IEEE, Oct. 2018, pp. 1–4. doi: 10.1109/CSNET.2018.8602974.

[6] Dr. Y. Perwej, N. Akhtar, N. Kulshrestha, and P. Mishra, ‘A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends’, vol. Volume 09, p. Pages 346-371, Jan. 2022, doi: 10.6084/m9.figshare.JETIR2201346.

[7] ‘Classifying Security Attacks in IoT Using CTM Method | SpringerLink’. https://link.springer.com/chapter/10.1007/978-3-030-53440-0\_32 (accessed Aug. 05, 2023).

[8] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, ‘Cyber Security Awareness, Knowledge and Behavior: A Comparative Study’, *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.

[9] S. Gautam, A. Malik, N. Singh, and S. Kumar, ‘Recent Advances and Countermeasures Against Various Attacks in IoT Environment’, in *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*, Coimbatore, India: IEEE, Mar. 2019, pp. 315–319. doi: 10.1109/ICSPC46172.2019.8976527.

[10] I. Ali, S. Sabir, and Z. Ullah, ‘Internet of Things Security, Device Authentication and Access Control: A Review’, vol. 14, no. 8, 2016.