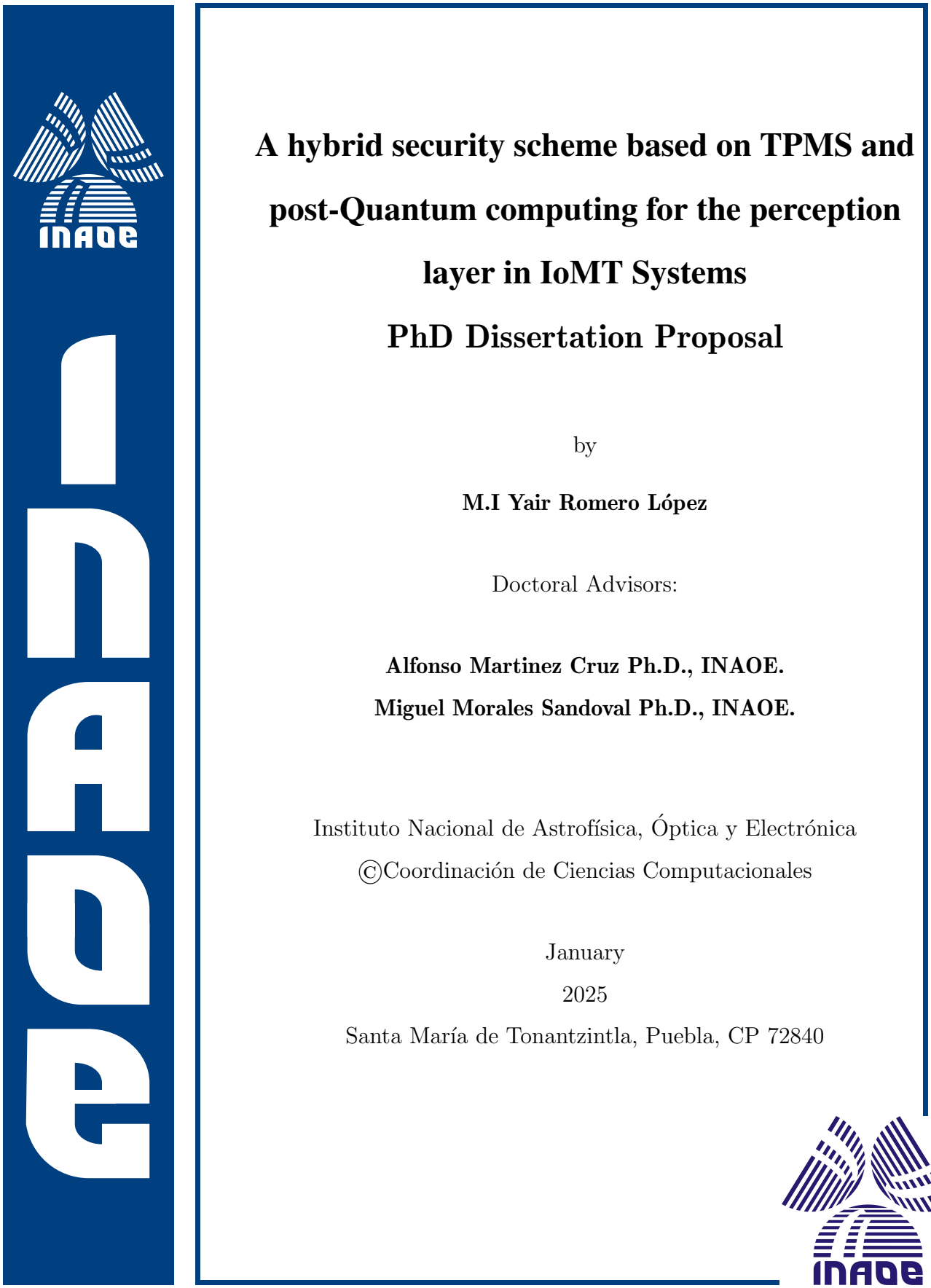

A hybrid security scheme based on TPMS and post-Quantum computing for the perception layer in IoMT Systems

PhD Dissertation Proposal

by

M.I Yair Romero López

Doctoral Advisors:

Alfonso Martinez Cruz Ph.D., INAOE.

Miguel Morales Sandoval Ph.D., INAOE.

Instituto Nacional de Astrofísica, Óptica y Electrónica

January

2025

Santa María de Tonantzintla, Puebla, CP 72840

Contents

Abstract

The security of IoT systems has become a priority area of interest owing to the growing demand for connected devices and the potential threats that they face. In this context, authentication plays a crucial role in verifying the devices' identity in communication, which is vital for mitigating the risks of infiltration by external attackers. However, IoT environments, particularly at the perception layer, present characteristic challenges, such as limited resource capacity, heterogeneity in communication, and device autonomy, which complicate the design and implementation of effective security schemes. The Internet of Medical Things (IoMT) represents an ecosystem in which devices, data, and applications collaborate to enhance health care. This approach is essential for ensuring patient safety, protecting highly sensitive data, and ensuring interoperability between systems, which are fundamental for safeguarding human lives. However, postquantum security can represent a solution to the threats posed by quantum computing to traditional cryptographic schemes. This approach focuses on implementing algorithms resistant to quantum attacks, such as those based on lattices, hash functions, and error-correcting codes, which offer secure alternatives against advances in quantum computing. In the context of IoMT systems, post-quantum security is key to protecting data and communications in resource-constrained devices and strengthening the resilience of these ecosystems against emerging threats. This thesis focuses on developing a new hybrid security scheme based on Trusted Platform Modules (TPMs) and post-quantum cryptographic algorithms specifically designed for the perception layer in IoMT systems. This approach considers the integration and collaboration of devices, data, and applications in medical environments, which directly influences the design of adaptive security schemes that address this domain's complexity and specific needs. Also, the scheme proposed addresses the resource limitations of devices as well as the diversity and scalability of systems. Furthermore, the proposed scheme will be implemented in a test environment representative of an IoMT ecosystem at the per-

ception layer, designing an embedded system with specific hardware components. Considering security and operational efficiency, its effectiveness and performance will be evaluated under real-world conditions. The results obtained are expected to significantly contribute to advancing knowledge in IoMT system security, providing a robust approach for protecting the integrity and confidentiality of data in these highly dynamic and challenging environments, which directly influences the design of adaptive security schemes that address the complexity and specific needs of this domain. A scheme is proposed that addresses the resource limitations of devices as well as the diversity and scalability of systems. Furthermore, strategies have been explored to mitigate the risks of external attacks such as the use of false identities or denial-of-service attacks. The implementation of the proposed scheme is carried out in a test environment representative of an IoMT ecosystem at the perception layer, designing an embedded system with specific hardware components. Its effectiveness and performance were evaluated under real-world conditions, considering both security and operational efficiency. The results obtained are expected to significantly contribute to the advancement of knowledge in the field of IoT system security, providing a robust approach for protecting the integrity and confidentiality of data in these highly dynamic and challenging environments.

1 Introduction

The Internet of Things (IoT) has emerged as a transformative and innovative technology with the potential to revolutionize various aspects of our daily lives. However, the exponential growth of IoT devices has brought about several security challenges. In this context, diverse ecosystems in these systems underline the importance of establishing a security scheme in the perception layer that includes devices or sensors. This layer represents a critical attack surface that requires special attention in terms of security [1]. Security at the perception layer of IoT devices is crucial, especially in critical environments, such as healthcare and vehicle control, where the focus is on preserving human life. Data can be manipulated if this layer is not protected, threatening vital decisions. For example, in the Internet of Medical Things (IoMT), security is essential for protecting the integrity and confidentiality of patients' medical information. Any vulnerability can expose data to manipulation or unauthorized access, compromising patient privacy and security. Therefore, implementing strong security measures in this layer is essential for maintaining trust in IoMT systems and protecting medical information from potential threats [2]. The IoMT is crucial in the perception layer, transforming how we interact with the environment. This technological revolution transcends convenience, health, and safety; IoMT could be the difference between life and death. Equipping everyday objects with smart sensors allows for the constant and accurate monitoring of vital variables, from air quality to heart rate. Collecting data in real-time and detecting anomalies early is essential in critical situations, such as detecting health problems or rapid response to medical emergencies. In this sense, the IoMT promises greater efficiency and convenience and unfolds unprecedented potential to save lives by providing an advanced and proactive perception layer in our physical environment. Recent research in quantum computing presents a considerable risk to the security of IoMT systems, as demonstrated by the wide array of protocols employed in the Internet of Medical Things (IoMT) [3]. Quantum algorithms, such as Shor's and Grover's algorithms,

the quantum Fourier transform, quantum walk algorithms for search-related issues, and adiabatic quantum algorithms for optimization tasks, have shown the capability to quickly factor large integers and solve discrete logarithmic problems, significantly speeding up these processes [4]. The expected computational breakthroughs of quantum computers are highly anticipated, especially in domains reliant on simulation and optimization tasks. However, their capacity to solve certain mathematical problems that classical computing systems cannot efficiently tackle poses a serious threat to contemporary asymmetric cryptography, such as RSA. Given the high probability that quantum computers capable of running Shor's algorithm will emerge within the next decade, pursuing alternative cryptographic methods has driven the advancement and standardization of post-quantum cryptography (PQC)[5]. In response to the imminent threats posed by quantum computers, global standardization and normalization organizations are actively developing new post-quantum (PQ) cryptographic alternatives. Currently, the most recognized body in this field is the National Institute of Standards and Technology (NIST), which plays a key role. NIST began its standardization project in 2016, and in August 2024, announced candidates that advanced to the fourth and most recent rounds [6]. These algorithms—CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON— were designed to address various cryptographic requirements. CRYSTALS-Kyber, for example, is optimized for general secure communications, such as encrypting website. In contrast, CRYSTALS-Dilithium, SPHINCS+, and FALCON focus on securing digital signatures, which are critical for verifying the authenticity and integrity of digital communications. Each algorithm has undergone rigorous testing and scrutiny, and their inclusion in forthcoming standards represents a significant step forward in the pursuit of quantum-resistant cryptography. The algorithms mentioned earlier belong to conventional computing, and must be adapted and migrated to systems with specific tasks, such as embedded systems. This is particularly relevant in the context of IoMT, particularly in the perception layer, which is the focus of this study. In this layer, it is necessary to migrate these algorithms to ensure the security of the de-

vices involved. On one hand, devices can leverage more secure architectures through hardware separation and trusted hardware and software. Specifically, Trusted Platform Modules provide a root of trust and a wide range of cryptographic functions, which is why tech giants such as Microsoft now mandate a TPM in every new system [7]. However, the migration of post-quantum algorithms with the help of pseudorandom numbers from TPMs, as a principle of secure hardware, offers an alternative to complement post-quantum security. Given the importance of both aspects in enhancing overall system security, this work explores them within the context of quantum threats [8].

This proposal is organized as follows: Section 2 introduces key concepts to provide the reader with a foundational understanding of the topics discussed, including IoT concepts, architecture, and the security service objectives of the perception layer. Section 3 reviews the state of the art in IoMT security, specifically in the perception layer. Section 4 defines the research problem, while Section 5 outlines the research objectives. Section 6 presents the methodology to be employed. Finally, Section 7 discusses the preliminary results, and Section 8 provides the conclusions.

2 Background

This chapter delves into the background and introduces the concept of IoT and IoMT, the prevalent architecture. It analyzes the components and functionalities within this architecture's layers, and then proceeds to examine security issues, particularly focusing on the perception layer, which is the primary focus of this thesis.

2.1 Internet of Things paradigm

The Internet of Things (IoT) refers to the virtual identification and representation of objects in a structure similar to that of the worldwide web. This notion was proposed by Kevin Ashton in 1999, who addressed the challenge of efficiently locating products such as lipsticks that were quickly sold out, making them difficult to obtain in conventional stores. Under Ashton's direction, the AutoID Center at MIT promoted the dissemination of the concept [9]. Radio frequency identification (RFID) technology plays a crucial role in this area. At MIT's Auto-ID Center, RFID was seen as an essential component for developing the IoT. However, RFID, while providing an identification method, is essentially indistinguishable from other forms of identity encoding. With the advancement and diversification of IoT applications, its scope is expanding to include sensor networks where devices collect data from the environment and transmit it to processing centers for analysis and subsequent applications [9]. IoT systems establish a connection between physical and global networks. IoT operates by linking real-world interfaces with the Internet, such as sensors collecting data and actuators intervening in the environment. These systems provide the technology necessary to instrument, quantify, and modify the physical world. Integrating sensors into the network adds data from the physical world and, in a sense, gives the Internet a dimension of consciousness. This addition represents a transformative change by closing the gap that has historically existed between the physical and virtual/cyber worlds, since the dawn of computing. In essence, the IoT

enriches the Internet by incorporating physical reality, turning it into a network encompassing people, information, services, and objects; in other words, the Internet of Everything. Kevin Ashton, IoT pioneer, noted: "In the 20th century, computers were mindless brains: they only knew what we told them. In the 21st century, thanks to the IoT, computers can perceive the world by themselves" [10].

Figure 1: IoT connects different devices [11].

With the advancement of IoT and its multiple applications, its scope is expanding, and it can now be based on sensor networks," things," where devices collect data and send it to processing centers for analysis and subsequent applications. These "things" encompass many interconnected devices, from commonplace household items like TVs and refrigerators to sophisticated sensors, as depicted in Figure 1.

There is no formal and commonly accepted definition of IoT. However, the concept can be described by an IoT architecture. Several different IoT architectures have been proposed in the literature, which are discussed below.

Main layers of an IoT architecture

This section presents a series of IoT architectures with layered structures and describes the three layers proposed in most currently implemented architectures. The components and descriptions of each layer were analyzed. Based on how the IoT processes data, it can have three logical layers: perception, network, and application (sometimes called the processing layer), as shown in Figure 2.

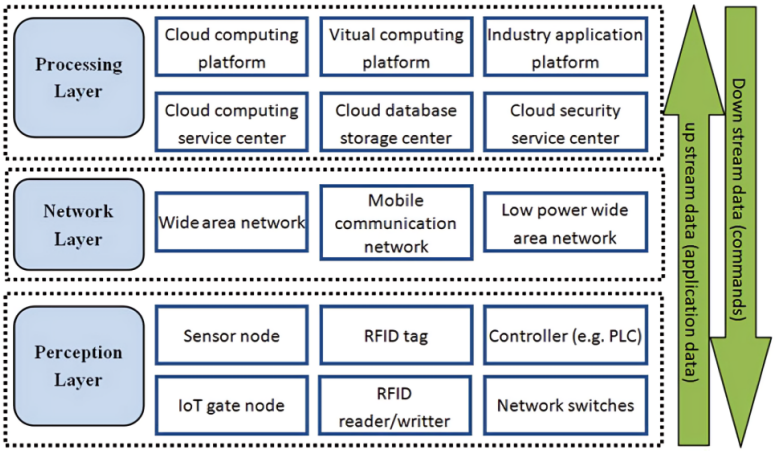

Figure 2: The basic three-layer architecture of IoT [12].

The perception layer

The perception layer is the physical layer that is used by sensors to detect and gather environmental information. It senses some physical parameters or identifies other smart objects in the environment [13]. The devices in this layer may include sensors for temperature, humidity, pressure, motion, light, and sound. These sensors can be embedded in everyday objects such as smart thermostats, security cameras, health devices, and connected vehicles, shown Figure 3. The IoT perception layer is crucial for providing real-time data on the state and behavior of the physical environment. These data are then used by other layers of the IoT system, such as the communication and application layers, to make decisions, perform actions, or generate helpful

information for end users. In addition to physical devices, the perception layer of IoT also includes some local area networks, including wired LANs (e.g. Ethernet, Fieldbus, Profibus) and wireless LANs (e.g., ZigBee,1 Bluetooth, WiFi, LORA.2). These networks are used to connect the IoT devices in the perception layer locally. With the development of IoT, more devices will be classified as being in the perception layer. Sometimes, the same kind of device can be classified as a perception layer device, a network layer device, or an application layer device, depending on the functionalities and services that it provides [14][15].

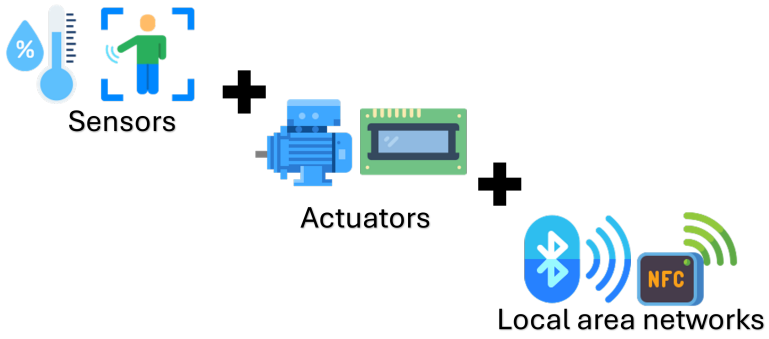

Figure 3: The main elements contained in the perception layer.

The network layer

The network layer connects to other smart things, devices, and servers. Its features also transmit and process sensor data [13]. The network layer of IoT describes the means of long-distance data transmission from the data collection venue to a data processing center. So, the network layer comprises traditional wide-area networks (WANs) and wireless WANs. Recently, a new type of wireless WAN has been developed targeting IoT applications: low-power wide area networks (LPWANs). Typical LPWAN networks include NB-IOT, LoRa, and SigFox; they have been widely constructed with commercialized operation [14]. In addition to the network infrastructure, connectivity capability may include devices such as routers, gateways, and hubs

that facilitate communication between devices with different connectivity technologies or communication protocols. The connectivity capability in IoT is essential for establishing a communication infrastructure that enables the interconnection of all devices and systems in the IoT ecosystem, thus facilitating the collection, exchange, and analysis of data for smart applications and connected services.

The application layer

The application layer is responsible for delivering application-specific services to the user. It defines various applications in which the IoT can be deployed, such as smart homes, smart cities, and smart health [13]. The processing layer, also known as the application layer, provides services and data for diverse applications. It is typically implemented via cloud computing platforms. It comprises platform infrastructure (hardware, software, and operating systems such as Hadoop), computing services (virtualization, NaaS, SaaS, and SecaaS), and database services (MySql, NoSQL) [14]. In addition, dashboards are used in this layer, which are fundamental tools in IoMT because they allow users to visualize and quickly comprehend data collected by connected devices. These dashboards provide an intuitive graphical interface that displays real-time information on the status and relevant environmental or operational data. The processing layer user interacts with relevant data and essential services, encompassing data and computational functionalities, and interfaces with diverse applications. Consequently, this layer can be divided into a data-processing unit and an application segment, handling user administration, service delivery, and interaction with various applications.

2.2 Internet of Medical Things (IoMT)

Smart healthcare is a framework that uses technologies such as wearable devices, also known as the Internet of Medical Things (IoMT), sophisticated machine learn-

ing algorithms, and wireless communication technology to seamlessly access medical records, link people, resources, and organizations, and then effectively manage and react to the demands of the healthcare environment in an intelligent manner [16]. The IoMT is an integral part of the IoT ecosystems, with architectures compatible with smart healthcare solutions. Protecting the integrity and privacy of information, such as patient medical data, in these environments is essential. Therefore, implementing robust security measures in the corresponding layer is critical to maintaining trust in IoMT systems and protecting information against threats. Adaptive solutions play a key role in ensuring the security of this technology, which represents 40% of the IoT market in 2020 and is projected to reach a value of $254.2 billion by 2026. It should be noted that tampering with devices in the perception layer could endanger patient lives, highlighting the importance of ensuring their proper functionality and security [17].

Security issues in IoMT perception layer

The perception layer in IoMT is vital, as it collects sensitive medical data and is highly vulnerable to physical and cyber threats. Ensuring its security is crucial to protecting patient privacy, maintaining data integrity, and preventing system-wide attacks. Our research focuses on this layer owing to its critical role and the lack of dedicated studies in the IoMT ecosystem, aiming to address this gap and enhance healthcare system reliability. Integrating connected devices, sensitive medical data, and critical healthcare systems presents significant security challenges, particularly in maintaining data confidentiality, integrity, and the availability of cyber threats. IoMT devices often operate with limited computational resources, making implementing advanced encryption and encryption protocols challenging. In addition, the extensive deployment of these devices expands the attack surface, exposing them to risks such as unauthorized access, data breaches, and manipulation of critical med-

ical functionalities. Figure 4 highlights some of the key challenges addressed in this study.

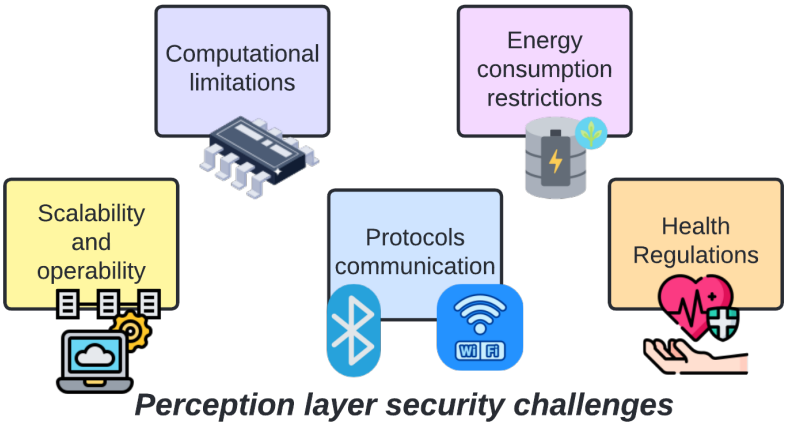

Figure 4: The main elements contained in the perception layer.

To overcome these challenges, organizations must adopt various security measures [18], including:

- **Encryption**: Ensure that data are encrypted during transmission and storage to prevent unauthorized access.
- **Access Controls**: Limiting access to IoMT devices and their data exclusively to authorized personnel.
- **Authentication and Authorization**: Verifying and authorizing devices before allowing them to connect to the network or interact with other devices.
- **Regular Updates**: Keeping IoMT devices up-to-date with the latest security patches and software updates to address known vulnerabilities.
- **Monitoring**: Continuously tracking networks and devices for unusual activities and responding promptly to security incidents.

2.3 Basic security services in the layer perception

IoMT devices exhibit various characteristics, functionalities, and communication methods in the perception layer. Sensors collect environmental data, actuators perform commands based on subsequent data, and IoMT gateway nodes and other network devices transmit data, whether processed or not. Consequently, IoMT devices can become targets of network attacks. The security requirements for IoMT devices must consider the devices themselves and the data they process. Consequently, security threats to IoMT devices can encompass various attacks, including both software- and hardware-based attacks. Therefore, it is crucial to protect information against cyber-attacks, as it represents a valuable resource. To ensure security, it is necessary to protect it from unauthorized access (confidentiality), ensure that it is not improperly altered (integrity), and ensure that it is only available to authorized parties when necessary (availability) [19], shown a taxonomy of security goals that include se service security denominated CIA.

Confidentiality: In IoMT ensures that only authorized users or nodes can access information and prevent unauthorized access. This involves protecting the content exchanged between nodes, such as preventing eavesdropping on wireless sensor networks. Strong encryption and authentication are used to address the confidentiality challenges. Confidentiality is also crucial in IoMT due to numerous users, devices and services sharing heterogeneous networks or ecosystems. Techniques such as privacy-preserving data publication (PPDP) are used to sanitize the data before publication. Encryption, a cornerstone of IoT security, such as through public key infrastructure (PKI), is used to obscure information, ensuring that only authorized users can securely access sensor node data and that the key distribution is secure. This robust security measure significantly improves the resilience against unauthorized access to network traffic. The following confidentiality requirements must also be satisfied [20].

- Only authorized users should be allowed to read the sensor node's information.
- The key distributions should be greatly secure.
- In order to achieve security against the traffic analysis attack, the public key and sensor identification needs to be encrypted.

Integrity: The integrity service allows only authorized modifications or prevents unauthorized modifications. Attackers capture nodes that prevent proper communication between them. Later, the attackers created a new connection that acted as a node. Data integrity is a service that allows clients of any network to recognize the exchange of altered communication content or to ensure that the content exchanged in the communication is not false, similar to information replication. The main focus of integrity is to ensure that the data content is not altered or compromised by third parties. If there is an attack and the system is compromised, recognizing its authentication can alter or corrupt the information, causing IoMT applications to malfunction.The opposite of integrity is alteration. Integrity attacks (hash collisions, man in the middle, birthday attack) and possible solutions (Hashing, message digest, message authentication code) [20].

Availability is a service that makes nodes in the perception layer available when authorized users need them. Data packets could be intercepted and redirected to another place when this service is not achieved. For example, DoS attacks may occur and intercept the packet between the router and another node that is not authorized, which would affect the communication network of the IoMT system, causing some nodes to be no longer available to the network user, triggering loss of information, and thus incorrect operation [13]. The availability of services ensures that the services and functionality are available even when the network is attacked. In the IoMT, most services in real-time are required. If the request is not attended to in a timely manner owing to the unavailability of any service, the services cannot

be rescheduled. Therefore, availability is a vital security requirement for the IoMT [20].

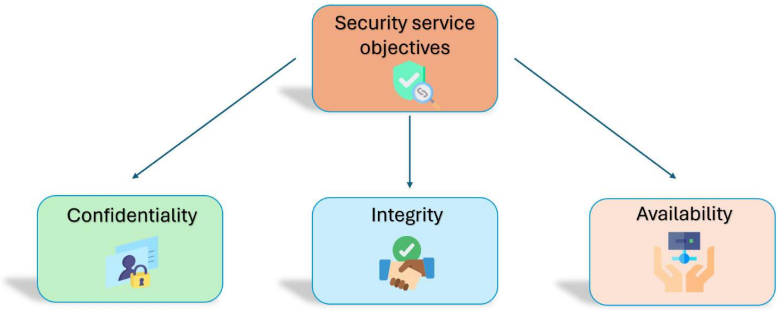

Figure 5: Taxonomy of security goals - CIA.

Each layer of the architecture requires a scheme that satisfies the requirements of the security services described above. Although each layer faces different attacks, this thesis focuses on security in the perception layer, for which we describe a classification of the main attacks and their description.

2.4 Types of attacks on the perception layer

There are classifications of main attacks given in the perception layer; two classifications are proposed, and further, some common attacks are described.

Physical adversary: One of the most potent assumptions is that an adversary has physical access to an IoMT device. Attacks that have access to some physical nodes and can make modifications are called physical attacks. The first type of physical attack is the SCA attack (Side Channel Attacks), in which the attacker takes advantage of the information obtained through secondary means, such as the device's power consumption or electromagnetic interference, to obtain sensitive information, such as encryption keys or confidential data. The second type of physical attack is the usual fault analysis attack, produced from interference deliberately introduced

by the attack. The interference can be voltage logic or noise signals to violate the security algorithm. In the present study, we focus on attacks based on weaknesses in the software or hardware implementation of cryptography algorithms [21][19]. There are some alternatives for extracting firmware from IoMT devices, which are considered physical attacks. The system's security is compromised through physical communication ports in these attacks. One alternative is the Joint Test Action Group (JTAG), an international standard test protocol used to program, debug chips, and explore ports [15].

Remote software adversary: Suppose the attacker can remotely alter the device's firmware. In this case, the objective is to identify weaknesses in the underlying software of IoMT devices to obtain unauthorized access or perform malicious actions. Attackers can exploit known or unknown vulnerabilities in the IoMT software for devices to infiltrate them and take control; there may even be a case where a device is hijacked, and that node is used to use it in malicious activities such as malware distribution. Some remote attestation (RA) techniques aim to detect malicious changes in device firmware by requesting a test to verify the device's integrity [15].

Active attacks: The attacker intercepts the connection and system resources to affect the normal operation of the device and thus modifies the information. Attackers gain unauthorized access to not only hack information but also damage and disrupt a node's communication [22]. Active attacks damage system resources. They are more harmful than passive attacks because malicious acts are carried out against data confidentiality, integrity, and availability [23]. The impact of active attacks is visible to victims. Therefore, this type of attack can be detected.

Passive attacks: Occur when the attacker intercepts information that passes to read and explore it. Here, the attacker's objective is to steal information without altering or modifying it; confidentiality is threatened. In most cases, the system resources are not influenced by passive attacks. For this reason, victims are often unaware

of passive attacks that are not directly visible. Therefore, there is less chance of detecting these types of attacks [22]. There are techniques to detect these attacks because even though there are no alterations in the information, there could be minimal alteration in the device's energy consumption. As can be seen, it is difficult for the victim to notice these small alterations.

Specific perception layer attacks

The most common attacks on the perception layer are analyzed below. These attacks fit some of the classifications described above.

Jamming: Occurs when an attacker blocks signals to prevent devices from communicating with each other and with the server [19]. Disrupting Wi-Fi or GPS signals is very easy and inexpensive. Radio interference disrupts network operations, and can cause message collisions and channel flooding. Interference severely affects data communication and results in unpredictable system responses [22].

Man in the Middle (MITM) Attack: The attacker intercepts the original communication between two nodes (usually between the client and server) and plays the role of a proxy user by establishing a new connection. In the IoT environment, an MITM attack occurs between an IoT device and a user interface application or a web server, as shown in Figure 6. The attacker can turn off all standard security implementations in the middle of the communication nodes. Some communication protocols commonly used in the perception layer, such as Bluetooth and Wi-Fi, are vulnerable to MITM attacks [22].

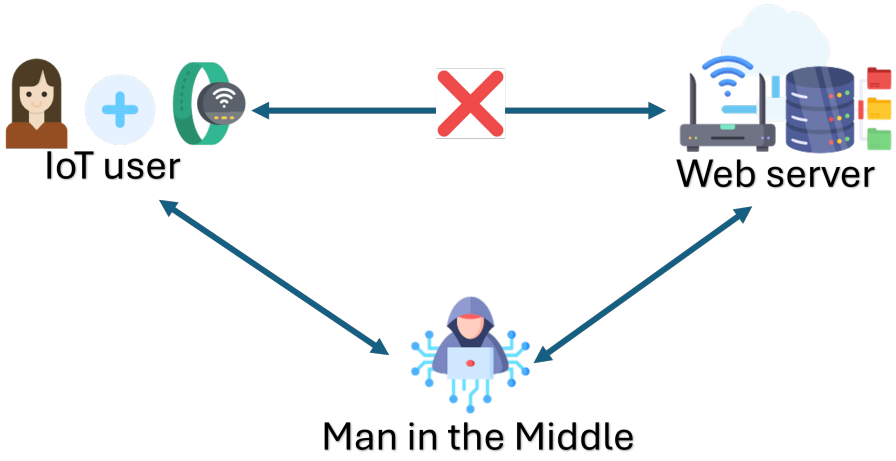

Figure 6: Man in the Middle Attack.

False Data Injection Attack: This attack is especially relevant in control and monitoring systems, such as those used in critical infrastructure, industrial systems, and sensor networks. An attacker attempts to modify data transmitted on a system or network by introducing false or manipulated information. In a false data injection attack, an attacker can compromise data integrity by manipulating the values transmitted by sensors or devices on the network. For example, in a power plant control system, an attacker could modify data from sensors that monitor temperature or pressure, leading to incorrect or harmful decisions by the control system.

Node Tampering: The attack involves replacing nodes or damaging sensors and actuators. It can be triggered by modifying the hardware or firmware of a device. When this attack occurs, the attacker can access the connected nodes to obtain sensitive and confidential information, jeopardizing the integrity and confidentiality of the data transmitted in the network. It is important to implement physical security measures such as data encryption, device authentication, and constant monitoring for signs of tampering or suspicious activity on the network to stop node manipulation. Many researchers have deployed swarm-based defenses to detect tampering [22].

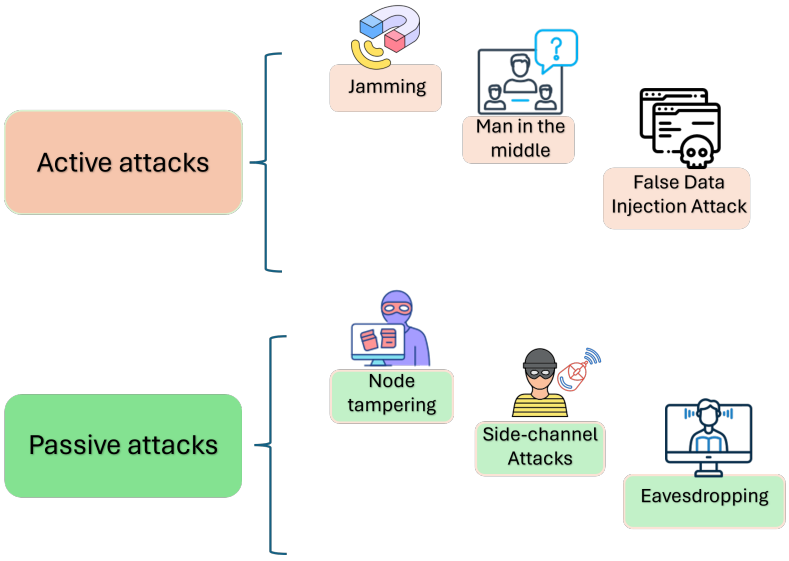

Figure 7: Classification of attacks in the perception layer.

Figure 7 shows the classification of the attacks mentioned above. It is important to mention that there are a significant number of attacks, and their growth depends on the technological demand and increasing number of nodes in all layers of the IoT architecture.

As discussed in the previous section, security vulnerabilities are traditionally classified in classical computing. However, quantum computing introduces significant challenges to the security frameworks of IoT systems, encompassing all ecosystems, particularly the IoMT ecosystem, which is our focus of interest; this topic is explored further below.

2.5 Security post-quantum environment

The recent emergence of quantum computing has required measures to maintain data security and integrity against emerging quantum threats. Quantum attacks targeting the perception layer encompass jamming, DDoS, and quantum desynchronizing attacks. Desynchronizing attacks include quantum faked state attacks and

quantum Trojan horse attacks, as described by Makarov and Hjelme [24]. Jamming attacks, such as Wireless Sensor Networks (WSN), typically occur in the perception layer. These attacks crash the communication medium by sending many requests to the server or alternating communication to block responses to reach the destinations [25]. The quantum version of this attack uses the entanglement property between the qubits sent to alter the communication and listen to traffic. The entanglement property allows each entangled pair of qubits to correlate their output states. These outputs are the measurements used to determine the encryption key among communication channels. This speeds up capturing the encryption key, which allows attackers to send many requests to the server to harm the communication channels [26]. A survey was conducted on IoT's significant threats and challenges in the post-quantum world. In this study, the author introduced a jamming attack targeting the perception layers of IoT devices, known as a quantum desynchronizing attack. This attack deploys maliciously entangled qubits to disrupt the communication medium between interacting parties, damaging Wireless Sensor Networks (WSNs) and rendering them unable to transmit or receive data [27]. Quantum DDoS attacks operate similarly to classical DDoS attacks, but the difference is that the quantum version uses malicious qubits in a superposition state. These results in the autonomous sending of malicious data that the perception layers cannot manage, rendering them unable to send or receive information and blocking their secure connections. It is important to note that, in the perception layer, DDoS attacks are frequently carried out due to the nature of the devices or sensors in this architecture. The proposed security solution counteracts quantum DoS attacks in two stages. First, it employed a quantum protocol to ensure secure communication in the data plane. Subsequently, a machine-learning-inspired ensemble classifier was designed to detect DDoS attack traffic in the control plane [28]. Although the above primarily pertains to IoT, it is important to note that it can be extended to ecosystems such as IoMT. Currently, most related works are specialized in IoT. As highlighted in this section, addressing current and future threats in IoMT systems is essen-

tial. Incorporating a hybrid security scheme that combines classical and quantum cryptography in the perception layer of an IoMT system offers a robust solution to protect sensitive data against both present and emerging threats. This layer, comprising sensors and resource-constrained devices, is particularly susceptible to attacks aimed at intercepting, manipulating, or falsifying critical medical information. A hybrid scheme integrates Post-Quantum Cryptography (PQC) algorithms that have been optimized to be lightweight and adapted to the limitations of IoMT devices. Furthermore, including a Trusted Platform Module (TPM) provides an effective means to enhance security by enabling robust mechanisms for authentication, secure key storage, and cryptographic data generation. Additionally, leveraging the TPM to generate pseudorandom numbers to support PQC algorithms further strengthens the security framework. This approach facilitates a seamless transition toward quantum-resistant cryptography, ensuring data confidentiality and integrity while delivering a sustainable and secure solution for critical medical systems where precision and privacy are paramount.

3 State-of-the-art

In this section, research is conducted that mainly describes works related to the security schemes of IoMT devices in the perception layer. A brief analysis of the techniques used was carried out, and some of their advantages and disadvantages were presented. It is worth noting that the term "IoT" is included as a keyword in the construction of this section due to the limited availability of topics that specifically address security within IoMT systems. Additionally, an analysis is conducted on both the currently implemented security schemes and post-quantum security approaches, as this thesis emphasizes a hybrid scheme. In the current digital age, the IoT has emerged as a solution to facilitate certain aspects of daily life, as how we interact with the world around us has changed thanks to this type of technology. Because there are various security challenges, it is important to recognize the concept of IoT, which can be adequately described through an architecture through the various processes that information undergoes, including data collection, data transmission, and data processing and applications. An IoMT architecture undoubtedly includes these processes, making it the most popular three-layer IoMT architecture [12].The perception layer deals with hardware components such as radio frequency identification tags (RFID), cameras, sensors, and wireless sensor networks (WSN).The literature states that protecting hardware devices is at the core of IoMT security. This suggests that IoMT security can be achieved only if the underlying hardware devices are secure. However, only some studies have focused on this layer of the IoMT architecture and its security [29]. In the perception layer, IoMT devices can be targets of network attacks, the most common of which are the following: Energy consumption attacks and denial of service (DoS) attacks, in the same way, IoMT devices can be captured basically and analyzed in a laboratory, in the same way, IoT devices may have been controlled by intruders [12]. For this reason, the security analysis of IoMT devices with strict protection schemes takes a long time, and it is difficult to find vulnerabilities, which is why the analysis of vulnerabilities in

the perception layer, given its heterogeneity, takes into account the hardware, communication protocol, and firmware used [15].In technical research, more and more applications are being developed for IoMT devices. The approaches and applications of the various technologies used are very different. With the increasing number of networked devices and the increased exchange of data, security and data protection in the IoT are critical aspects for research [30]. Each layer of IoMT design has its own security vulnerabilities, the most common security categories at the perception layer include:

3.1 Trusted Platform Module - TPM

To accommodate weak connections and changes in network topology, [14] proposed a Task-Oriented Authentication Model (ToAM) for UAV-based networks employing Blockchain and PKI technology. In ToAM, UAVs were equipped with TPM chips to securely store data and used TLS handshakes were used to prevent common attacks against software-only. Furthermore, the authentication mechanism consisted of two phases: authentication for group construction and intra-group authentication, with hash values stored in the Blockchain representing authentication data. The authors in [14] presented a secure and globally operational UAV authentication system based on trusted security mechanisms and established protocols; however, this approach does not guarantee that UAVs connect to a trusted environment. In this study [31], an ECC-based solution was proposed to protect the perception layer of IoT devices, addressing DDoS, botnets, and spoofing attacks by directly applying ECC over binary fields to secure the perception layer in mobile phones and ATM cards used for electronic payments, there are some drawbacks such as the encryption and decryption time on ATM cards being more extended than that on mobile phones owing to limitations in processing capacity, which affects the jitter value in digitals system.

3.2 PUFs

PUF can be used to increase hardware security. The main idea behind PUF is to use minor intrinsic variations created during the chip manufacturing process to create a unique identity for each device. This makes it a widely used security option because of how difficult it is to clone these types of chip properties [32], below is related work.The Bagua protocol [33] provides a comprehensive solution for improving the security of IoT devices by using Strong PUF technology, array encryption and anti-attack functions. This guarantees the integrity and confidentiality of data transmitted by IoT devices. It is also important to mention that the protocol's configurability and adaptability allow it to be customized to the specific requirements of different IoT devices. When implementing the protocol, considerations must be made regarding complexity, resource requirements and performance overhead.The study in [34] presents a demonstration of the concept of the JULIET-PUF, which performs a security analysis that shows an improvement in the security level of SRAM-PUF schemes, especially in the attack model appropriate for IoT devices. It is highlighted that the proposed method can significantly increase the security of IoT implementations based on SRAM-PUF without increasing their costs, and the limitations of the JULIET-PUF scheme proposed in this article have a possible impact on the useful life of the devices, owing to controlled power failures and the possible high engineering costs associated with implementation in the perception layer. In [35], different design approaches were investigated to improve the security of Physically Unclonable Functions (PUFs) against modeling attacks. Modeling attacks on Arbitrator-based PUF architectures were analyzed, highlighting the most suitable modeling algorithm for each design approach. In addition, the area efficiency of the studied PUF designs is examined, and optimal approaches are suggested for different area constraints, providing guidelines to accurately evaluate the security of PUFs and guide the PUF community towards best practices. This work does not address other factors that could influence the security of PUFs, such as resistance to

other types of attacks or scalability in real deployment environments. In addition, there is limited access to computational resources in nodes in the perception layer. This could be an important point to consider when evaluating the effectiveness of proposed design approaches.

3.3 Blockchain

Blockchain is a strong option for the security of IoT devices because of its immutability, decentralization, and transparency in the data transactions collected by devices. An example of these characteristics is found in the main contribution of this article [36], which focuses on proposing a security defense method for the Internet of Medical Things (IoMT) based on blockchain and fuzzy set theory. This proposal is implemented in the perception layer of IoT, which involves data collection through smart sensing devices. However, no performance metrics were provided to evaluate the node and its computational resources, as only the algorithm metrics were evaluated, making it unclear on which device it was performed. This suggests that a node in the perception layer sends information to the cloud to process the proposed algorithm. In [37] proposes a secure and trusted blockchain hardware architecture thanks to the reconfigurability of an FPGA. The goal was to realize the implementation of Blockchain in hardware adapted to an IoT device to improve physical and virtual security mechanisms on devices in a network. Some attacks are included, and the result was favorable. However, the limitations identified in the implementation of BIoTS (Blockchain-IoT) include the limited availability of resources in the FPGA, where the designed modules occupy 47% of the available logical units. This suggests that FPGA capacity could be a limiting factor in the implementation of more complex systems. Additionally, although not explicitly mentioned in the summary provided, there may be limitations to the scalability, power consumption, and processing speed of the algorithms implemented on BIoTS hardware. The study in[38]

introduces a machine learning AI algorithm that generates sidechain management with high security performance, making it suitable for secure real-time IoT applications. The algorithm optimizes the number of sidechains created to balance computational complexity and mining delays. However, it is not located in the perception layer. Integrating blockchain into networks at this layer can increase computational complexity, which may reduce the quality of service for real-time applications.

3.4 Cryptography algorithms

Cryptography algorithms optimize the data encryption transmission mechanism in IoT systems. In [39], the proposed security verification mechanism improves security using biometric fingerprint identification technology. Improves security protection performance of the IoT power perception layer. The system achieved a high identification accuracy rate of 99.75% in the simulation tests. However, its limitations may include potential challenges in scalability and deployment in large-scale energy IoT networks.

3.5 Post-quantum possible solutions

There are five quantum physical attacks on IoT devices, namely, node manipulation, code injection, brute-force attacks, and quantum attacks based on HHL and QKD techniques. Node manipulation is a security attack [24]. The attacker's goal is to capture sensitive information, such as the encryption key, that enables nodes to communicate with each other. The quantum version of this attack uses Shor's algorithm to break through physical security defenses and capture the encryption key by solving the factorization problem, thereby gaining physical access to the source code of the communication [40]. One potential solution is the use of TPM, which provides conventional cryptography and key storage, as outlined in the previous

sections. It offers security defenses against various types of attacks, including post-quantum attacks, as demonstrated in [8]. This approach presents a viable solution and will serve as a strong foundation for the work in this thesis. An enhancement will be made concerning the post-quantum algorithms selected for implementation in the system's MCU, and an extrapolation will be made to an IoMT ecosystem. The potential of blockchain technology to enhance data privacy and security in the Internet of Medical Things (IoMT) was underscored in [41], attributing its effectiveness to the decentralized, transparent, and immutable characteristics of the technology. This study highlights the critical role of post-quantum cryptography in mitigating quantum computing threats while acknowledging challenges such as scalability, interoperability with existing healthcare infrastructure, and integration of quantum key distribution (QKD). Furthermore, the resource constraints in IoMT devices present substantial obstacles to the adoption of these advanced solutions, emphasizing the need for continued research to address these limitations. The study [42] presented a secure authentication mechanism against quantum attacks for IoT applications in transportation systems based on a Post-Quantum Key Encapsulation Mechanism (PQKEM) using the CRYSTALS-Kyber algorithm selected by NIST. The proposed protocol aims to ensure the integrity and confidentiality of communications in IoT networks, which are vulnerable to attacks, such as data interception and manipulation. While this work is notable for its security formalization through the Or-Random model and a comprehensive performance analysis, it highlights limitations, such as the need for robust infrastructure to support post-quantum cryptography and the complexity of integrating the solution into existing systems, which may hinder practical implementation. The study in [43] examined an offloading scheme utilizing a Post-Quantum Edge Server (PQES) to handle the computationally and memory-intensive tasks of post-quantum cryptography (PQC). This approach enables IoT devices to operate efficiently by offloading cryptographic processes. The results show substantial reductions in resource consumption, with RAM usage reduced to 1.05 KB and CPU usage to 1.75%, allowing the PQES to effectively manage

1,000 concurrent connections. Nevertheless, a potential limitation of the scheme lies in its dependence on the PQ Edge Server; any downtime or performance issues with the server could jeopardize both the security and functionality of the IoT devices. The paper "PQCAIE" addresses the security challenges in IoT-based healthcare systems, particularly in mitigating quantum computing threats, by proposing the integration of Post-Quantum Cryptography (PQC) and TLS 1.3 to enhance authentication methods and safeguard sensitive health data. While emphasizing the advantages of increased resilience against quantum attacks, it also identifies significant limitations including high computational overhead, integration challenges with existing systems, and potential performance impacts. The study concludes by proposing solutions to overcome these obstacles to facilitate the development of more secure and reliable healthcare technologies [44]. In [45], the integration of Kubernetes with embedded systems in IoMT was investigated using Crystal-Kyber and ASCON algorithms. The findings demonstrated robust operational efficiency, with performance evaluations indicating key encapsulation and decryption times suitable for medical applications. Additionally, this study highlights the scalability and resource efficiency of cryptographic operations managed by Kubernetes, achieving low CPU usage on a Raspberry Pi-based master node. However, the research identifies certain limitations, including potential challenges in implementing the solution across diverse healthcare environments owing to variations in hardware capabilities and the complexity of system integration.

The table 1 provides an overview of additional works related to the state-of-the-art, analyzing various security techniques, along with their respective advantages and disadvantages.

Article	Proposed scheme	Related architecture layer	Limitations	Indicators	Ecosystem	Real/ Simulation
Sebastian Paul,et al (2021.)[2]	Integration of post-quantic cryptography with MBED TLS and trust platform modules (TPMS) to cease a safe environment on IoT devices.	Perception	*Limited hardware resources for PQC *Lack of implementation of modern hash functions in TPMS.	*The time performance of the Kyber and Sphincs+ PQC algorithms was evaluated in various hardware settings using TPM 2.0.	IIoT	Real
Balogh, S, et al (2021) [3]	Machine learning classifiers for intrusion detection systems in IoT.	Conectivity	*High costs of blockchain operations. *Blockchain's inability to prevent denial of service attacks on IoT networks.	*Score the performance of intrusion detection systems and machine learning classifiers in IoT networks.	IoT	Simulation
Venkata K. V, et al (2023)[5]	Integrates a TPM with a PUF to securely seal the PUF key inside the TPM and upload data to Tangle for device authentication.	Perception	*The need to guarantee the reliability of the PUF function, the complexity of intending the TPM with the PUF.	*Time and memory storage capability to securely seal and unlock PUF keys generated inside the TPM.	IoT	Real
A. Kama,et al (2023)[4]	This facility profiles a large number of IoT devices simultaneously, enabling the collection of high-circulation data for the PUF.	Perception	*The limitation of the method is that it requires careful control of the temperature during data collection to ensure consistent results.	*Hamming weight of samples from a specific device with different power failure durations to evaluate the quality of the generated CRPs.	IoT	Real

Table 1: Related works.

Discussion

In general, post-quantum security within the preparation layer of IoMT systems has not been studied in detail. Although various related works address security in IoMT, most focus on implementing solutions in higher layers of the architecture model, such as the application or communication layers, overlooking the specific challenges that arise in the layers closer to the hardware. Among these challenges, one of the most significant is the limitation of computational resources in medical devices, such as sensors, vital sign monitors, and wearable devices, which typically operate under constraints in energy, processing power, and memory. The need to protect the integrity and confidentiality of data from the lowest layers of the architecture is becoming increasingly critical in an environment where cyberattacks are growing more sophisticated, and the imminent arrival of quantum computers threatens to compromise traditional cryptographic schemes. However, implementing post-quantum cryptographic solutions in resource-constrained devices presents multiple challenges: existing algorithms are often too complex to be efficiently executed on constrained medical hardware, and reliance on solutions in higher layers

may introduce latencies or additional vulnerabilities.

Furthermore, few studies have conducted practical research in real-world environments, such as hospitals or home monitoring systems, where the heterogeneity of devices, network conditions, and real-time constraints complicate the adoption of robust security solutions. This highlights a significant gap between theory and practice, as many previous works have been limited to simulations or controlled evaluations without considering the dynamics and demands of real medical environments.

4 Research proposal

In this chapter we present the reasons that gave rise to the research, the hypothesis, the objectives that we set out to achieve and a brief summary of the contributions that were achieved as advances during this period.

4.1 Problem statement

Perception layer devices in IoMT face a limitation in computational resources, which creates difficulties in performing complex cryptographic security operations. Given the threat posed by quantum computing to classical cryptography, this resource scarcity is further exacerbated by the need to integrate post-quantum cryptography (PQC) schemes. In addition, Trusted Platform Modules (TPMs) have been used in perception layer devices to strengthen physical security, and these TPMs must support both classical and post-quantum security during the transition phase. This challenge implies that perception layer devices must balance the execution of demanding security operations with limited computational resources [8].

A hybrid scheme combines classical and PQC algorithms to ensure security during the transition to quantum-resistant standards. In resource-constrained IoMT devices, this approach balances compatibility, robustness, and efficiency by prioritizing PQC for critical operations while classical algorithms handle less demanding tasks.

4.2 Hypothesis

Generating a hybrid scheme using Trusted Platform Modules (TPMS) in an IoT system would significantly improve the performance by offloading computationally intensive operations, such as hash function calculations and the Random Number

Generator (RNG), to the TPM. This approach can reduce the computational overload on the microcontroller running the post-quantum cryptography (PQC) scheme in the IoMT perception layer. By leveraging the capabilities of the TPM to handle both classical and post-quantum security tasks, this hybrid solution can optimize resource usage in low-end devices while maintaining robust security against quantum threats.

Figure 8 presents a three-layer IoMT architecture, which is the focus of this thesis. The proposed security scheme will be implemented in the perception layer to ensure the protection of information generated by the IoMT embedded system before its transmission to the connectivity layer.

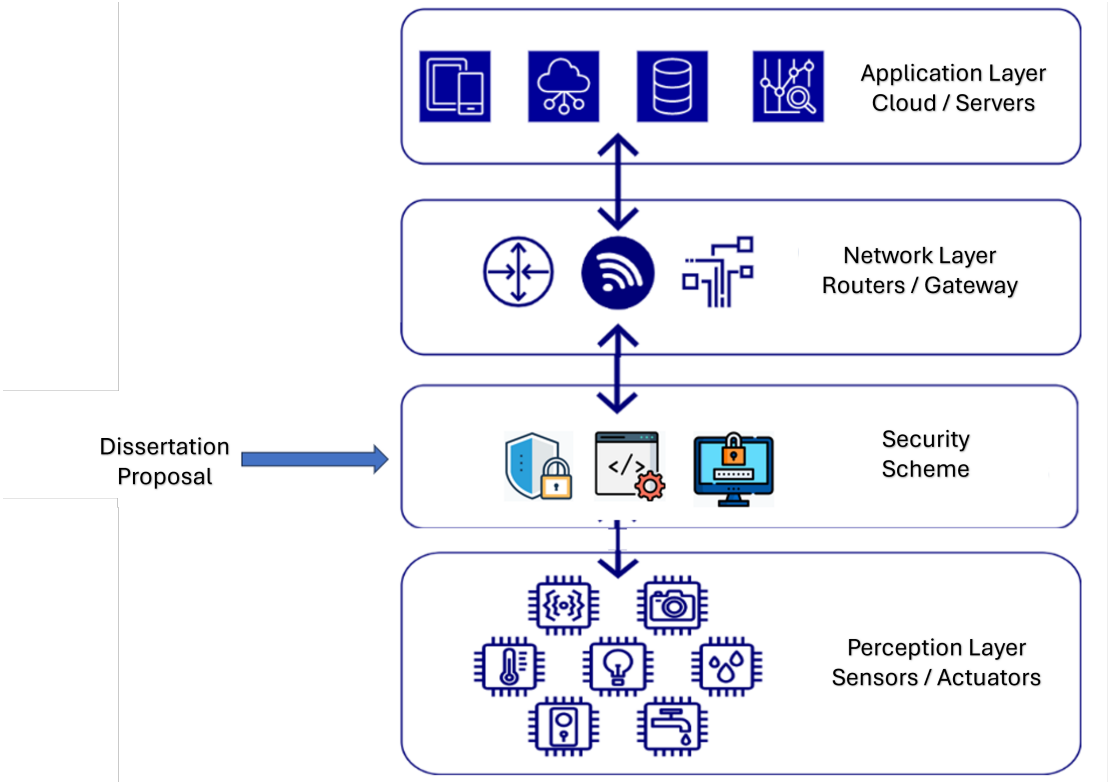

Figure 8: IoMT three-layer architecture implementing the proposed security scheme.

4.3 Objectives

General Objective

To develop a hybrid security system that considers the main limitations of IoMT devices, utilizing both classical and post-quantum cryptography (PQC) approaches to protect the perception layer from potential threats and ensure authentication, integrity, and confidentiality.

Specific Objectives

1. Analyze and adapt a cryptographic scheme evaluated by NIST and migrate it to an embedded system in the perception layer of an IoMT environment, integrating both classical and post-quantum cryptography approaches to ensure security.

2. Develop and integrate a method for Trusted Platform Modules (TPMs) to offload cryptographic operations, improving system performance and reducing the load on microcontrollers.

3. Design and implement a security system that addresses the resource limitations of IoMT devices, including limited processing power, high data traffic speed, and scalability.

4. Evaluate the effectiveness of the proposed hybrid system to protect the perception layer of IoMT devices from both quantum and classical threats, ensuring authentication, integrity, and confidentiality.

4.4 Research questions

- How does the integration of a hybrid cryptographic scheme (classical and post-quantum) affect the performance of IoMT devices in the perception layer?
- What are the implications of migrating post-quantum algorithms to low-performance IoMT embedded systems in terms of efficiency and security?
- In what ways does the use of Trusted Platform Modules (TPM) enhance the physical and logical security of IoMT devices in the perception layer?
- How can limited resources of IoMT devices be optimized when implementing hybrid schemes integrating both classical and post-quantum cryptography?

4.5 Methodology

In this research, a methodology composed of the following steps is considered:

1. **Hardware and TPM requirements in the IoMT Ecosystem:** In this initial stage, a detailed analysis of the security requirements for the IoMT perception layer is conducted, considering the limitations of embedded systems and potential threats. Additionally, tests will be performed with TPM modules on IoMT devices to evaluate resource consumption and its impact on overall system performance.
2. **Analysis and Selection of Cryptographic Algorithms:** Cryptographic schemes evaluated by NIST, especially post-quantum cryptography (PQC), will be reviewed to select the most suitable algorithms for integration into the system. A decision matrix will be used to weigh factors such as security strength, performance, and resource consumption.

3. **Adaptation and Migration to IoMT Embedded Systems:** The selected cryptographic algorithm will be adapted to fit embedded systems with limited processing power and memory. This will involve optimizing the algorithms for efficient execution on low-resource devices, while maintaining high levels of security. The migration process will focus on ensuring compatibility with the IoMT architecture, particularly within the perception layer, where real-time data collection and processing occur.

4. **Implementation of the Hybrid Security Scheme:** A hybrid cryptographic system will be designed and implemented, integrating both classical and post-quantum cryptography approaches. This system will leverage the strengths of traditional cryptography for immediate security needs while incorporating PQC for future protection against quantum threats. The hybrid system will be tested to ensure its efficiency, ensuring it meets the performance standards required for real-time applications in the perception layer.

5. **Integration of Trusted Platform Modules (TPMs):** Trusted Platform Modules (TPMs) will be integrated into IoMT devices to offload resource-intensive cryptographic operations such as hash functions and pseudo-random number generation (RNG). This phase will involve configuring TPMs to work seamlessly with the hybrid cryptographic scheme, improving the performance of the embedded system. Special attention will be given to ensuring that TPMs provide the necessary security improvements, such as the root of trust, while minimizing the impact on device performance.

6. **Evaluation of the Hybrid System:** The effectiveness of the hybrid cryptographic system will be evaluated through a series of tests designed to assess its ability to protect the IoMT perception layer from both quantum threats. Key security metrics such as authentication, integrity, and confidentiality will be measured. Additionally, resource consumption, performance, and scalability of

the system will be evaluated under various conditions, ensuring that it meets the practical constraints of low-performance IoMT devices.

4.6 Activities schedule

The table 2 outlines the semesterly activities planned over the four-year duration of the doctoral program. Activities already completed are highlighted in green, while those yet to be completed are marked in blue.

Year	2024		2025		2026		2027	
Activities/Semester	1	2	1	2	1	2	1	2
Review of related work								
requirements in the IoMT Ecosystem:								
Writing of the thesis proposal								
Period of classes								
Define the IoMT architecture and Post-Quantum								
Integration of Trusted Platform Modules (TPMs)								
Evaluation of the Hybrid								
Academic research stay								
Journal article								
Conference article								
Thesis Writing								
Thesis defense								

Table 2: Activities schedule.

5 Preliminary Results

As part of the preliminary work, progress on implementing and designing an IoT-embedded system with a Healthcare focus was developed. The IoT system was designed to measure and predict CO_2 concentrations in indoor environments, thereby

reducing the risk of COVID-19 transmission. This system identifies high-risk areas with poor ventilation, enabling informed decision-making to mitigate contagion. Additionally, a security mechanism was integrated into the perception layer of the IoT architecture to ensure data confidentiality and authentication. The IoT system, which uses classical algorithms for encryption and authentication, was implemented. This system is a preliminary stage aimed at evaluating the performance of security algorithms using a TMP in embedded IoMT systems. This evaluation provides a foundation for identifying the disadvantages and challenges that must be considered in the proposed solution and is intended to be addressed in the subsequent stages of the research. The data security scheme was implemented to ensure the confidentiality, integrity, and authenticity of information within the IoT system. This was achieved using the MQTT protocol and the Trusted Platform Module (TPM). This security framework protects critical data throughout the communication cycle, ensuring reliable and secure system operation. The process begins with generating secure keys and initialization vectors to establish a robust encryption framework. Sensitive data are then encrypted using the Advanced Encryption Standard (AES) algorithm. An authentication and integrity mechanism is also integrated using Hash-based Message Authentication Codes (HMAC), specifically generated with secure algorithms such as HMAC-SHA256. Finally, the encrypted data is decrypted at the receiving end, and its integrity is verified, ensuring that the information remains unaltered during transmission and is completely authentic. As a result, the work was presented at the EDIESCA 2024 congress, held in the city of Aguascalientes, Mexico, from 28 to 30 October. The work presented was titled "Implementation of a Security Scheme for an IoT System to Predict Indoor CO2 Levels and Mitigate COVID-19 Using Time Series Algorithms." In addition, we were invited to submit the article to the VLSI Integration Journal. The work follows this structure, detailing the security mechanisms implemented to ensure the data's confidentiality, integrity, and authenticity within the embedded system. The process consists of four main stages, as shown in Figure 9:

1. **Secure Key and Initialization Vector (IV) Generation:** A secure key and initialization vector are created to establish a robust encryption framework, ensuring the randomness and security required for the encryption process.

2. **Encryption of Sensitive Data:** Sensitive data is encrypted using the Advanced Encryption Standard (AES) algorithm to protect it from unauthorized access. This step ensures that only authorized parties can decipher the information.

3. **HMAC Generation for Authentication and Integrity:** A Hash-based Message Authentication Code (HMAC) is generated using secure hashing algorithms (e.g. HMAC-SHA256). This step provides both authentication and integrity verification, protecting against tampering or unauthorized modifications to the data.

4. **Decryption and Integrity Verification:** The encrypted data is decrypted upon receipt, and its integrity is verified using the HMAC. This step ensures that the data has not been altered during transmission and remains authentic.

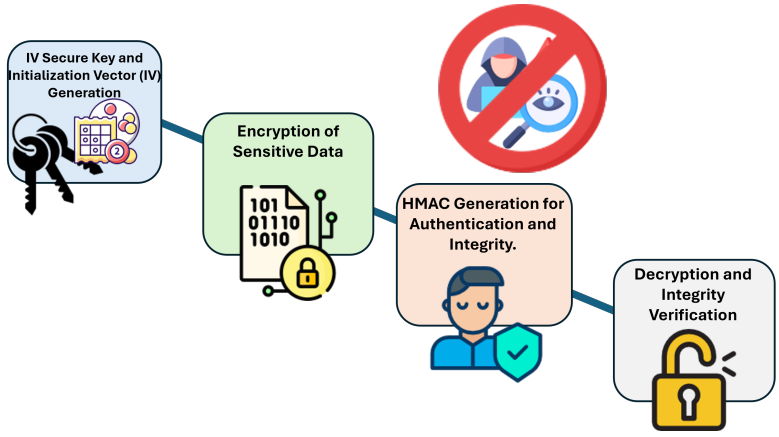

Figure 9: Encryption and Data Integrity Workflow.

A hardware-based TPM random number generator (RNG) was employed to produce cryptographically strong, unique IVs and AES keys for each iteration, significantly enhancing the algorithm's security against attacks. By performing these

critical operations directly on TPM, the integrity and confidentiality of the data were guaranteed. Furthermore, using TPM ensured that the generated cryptographic values were resistant to tampering, offering a robust solution for secure data handling in the system.

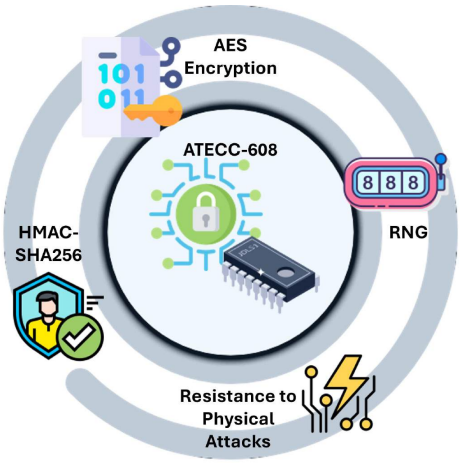

Figure 10: Security Mechanisms Implemented with TPM ATECC 608.

In these experiments, the ATECC608 TPM, shown in Figure 11, was utilized, and its hardware connection for communication with the microcontroller was established. A security algorithm was implemented in which the microcontroller used pseudo-random numbers generated by ATECC608. This approach serves as a precursor to the objectives of this study, particularly in the application of post-quantum algorithms.

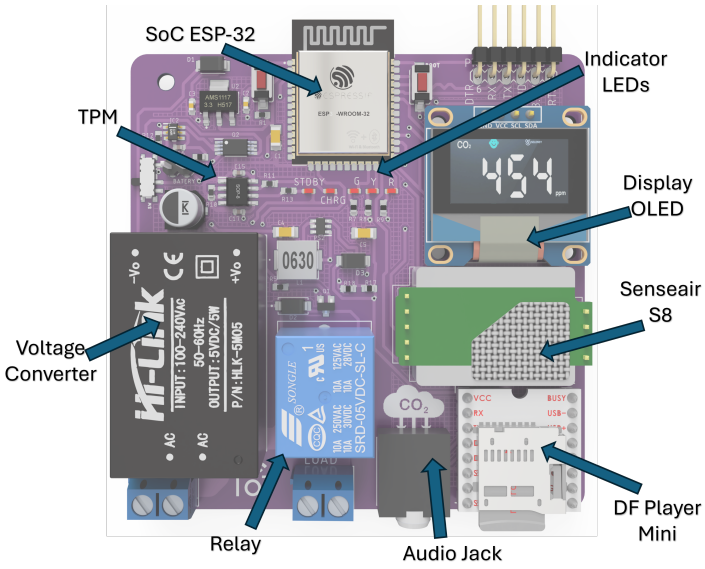

Figure 11: Embedded system design with a ATECC608 TPM.

The TPM ensured the security of cryptographic operations by generating robust and unique initialization vectors (IVs) and AES keys through its hardware-based pseudo-RNG. By performing these critical operations directly within the TPM, the system achieved enhanced data integrity, confidentiality, and tamper resistance, offering a highly secure encryption solution. The generated initialization vector is illustrated in Figure 12.

```
Generated IV: 24 2B 23 C3 63 3E 88 66 B4 C 6F F8 ED C2 4D 66
Generated AES key: F6 BD 3D B9 66 7A CC 52 FE 80 99 AB 5D 70 8C 6E
JSON string: {"C": 1041, "T": 24, "H": 22, "P": 978}
Encrypted text: CC D8 6B 76 17 DC 5D 74 74 25 FF 2A E8 AE EA EB 93 AC BE
Decrypted text: {"C": 1041, "T": 24, "H": 22, "P": 978}
```

Figure 12: Generation of the Initialization Vector and AES Key for encrypting the JSON transmitted from cloud.

As part of this experiment, an embedded system with the ESP-32 system-on-chip (SoC) serving as its core component, equipped with Internet connectivity, was developed. The system transmits data through a 2.4 GHz Wi-Fi network and inter-

faces with various peripheral devices. Among these peripherals is an OLED display, which provides real-time information on Internet connection status and CO_2 concentration levels, measured in parts per million (ppm) by the Sense-Air S8 NDIR sensor. Furthermore, the security framework was established using the ATECC-608 cryptographic module, which is integrated with the SoC through the I2C communication protocol. It is important to highlight the development of the embedded system shown in the Figure 11, which serves as a foundation for this research. During the course of the thesis, similar IoMT systems will be developed to enable testing in real-world environments. This approach aims to validate the proposed solutions under practical conditions and further refine their applicability and effectiveness.

Submitted Article

A work related to this research, titled: **"Implementation of an IoT system with a security scheme to predict indoor CO_2 levels and mitigate COVID-19 using time series algorithms"**, has been written and is currently awaiting acceptance in the *VLSI Journal*, a renowned journal focused on all aspects of VLSI (Very Large Scale Integration). The journal emphasizes cross-disciplinary collaboration in fields such as design, verification, testing, and applications of integrated circuits and systems, as well as related topics in process and device technology (December/2024, Impact factor: 2.2, Cite score: 3.8, `https://www.sciencedirect.com/journal/integration`). (Submitted December 26, 2024)

Publication plan

- The publication is planned for December 2025 in the IEEE Internet of Things Journal, (impact factor of 8.2, Q1)
- A conference paper, attending the 15th International Conference on Internet

of Things (IoT 2026)

- Attending the EAI International Workshop on Internet of Medical Things Security (IoMT 2027)

6 Conclusions

The critical challenge of securing the perception layer of the Internet of Medical Things (IoMT) systems, where IoMT devices face significant resource limitations and vulnerabilities to classical and quantum threats, has been addressed. This research focused on migrating post-quantum cryptography (PQC) algorithms to embedded systems while exploring the potential use of Trusted Platform Modules (TPMs) to offload cryptographic operations and enhance system performance. The hypothesis that integrating a hybrid security system, combining classical and PQC approaches, would improve performance by offloading resource-intensive operations to the TPM has been partially validated through preliminary results. The successful implementation of the ATECC608 TPM for generating secure pseudo-random numbers reduced the load on the microcontroller, thereby optimizing resource utilization. This preliminary work lays the foundation for future research on the potential of TPMs to provide both physical and cryptographic security in low-performance IoMT devices, particularly in the perception layer. These findings support the idea that embedding hybrid security schemes based on NIST-evaluated post-quantum algorithms, such as CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON, into IoMT devices with the assistance of TPMs can significantly enhance security and improve efficiency. This approach offers a viable solution for protecting critical data in environments increasingly vulnerable to quantum threats. Further testing and successful integration of these post-quantum algorithms into IoMT embedded systems are required to fully assess this hybrid security strategy's long-term effectiveness and benefits.

References

[1] A. K., M. Bouhlal, R. A. Abdelouahid, S. Filali, and E. H. Benlahmar, "Perception layer security in the internet of things," *Procedia Computer Science*, vol. 175, pp. 591–596, July 2020.

[2] M. Akhi, S. Memon, C. Eising, and L. L. Dhirani, "Machine learning for healthcare-iot security: A review and risk mitigation," *IEEE Access*, vol. PP, pp. 1–1, 12 2023.

[3] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. Ramírez Gutiérrez, and C. Feregrino, "Artificial intelligence for iomt security: A review of intrusion detection systems, attacks, datasets and cloud-fog-edge architectures," *Internet of Things*, vol. 23, pp. 1–82, 08 2023.

[4] A. Alomari and S. A. Kumar, "Securing iot systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," *Internet of Things*, vol. 25, p. 101132, 2024.

[5] M. Mosca and M. Piani, "Quantum threat timeline report 2020," 2021. Accessed: 2025-01-09.

[6] National Institute of Standards and Technology, "Post-quantum cryptography: Round 4 submissions," 2024. Accessed: 2025-01-09.

[7] Microsoft, "Trusted platform module overview," 2024. Accessed: 2025-01-09.

[8] S. Paul, F. Schick, and J. Seedorf, "Tpm-based post-quantum cryptography: A case study on quantum-resistant and mutually authenticated tls for iot environments," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES '21, (New York, NY, USA), Association for Computing Machinery, 2021.

[9] C.-K. Wu, *Internet of Things Security- Architectures and Security Measures*. Singapore: Springer Nature Singapore Pte Ltd. 2021, 1 ed., 2021.

[10] F. Hu, *Security and Privacy in Internet of Things (IoTs) - Models, Algorithms, and Implementations*. USA: CRC Press, 1 ed., 2016.

[11] H. Allioui and Y. Mourdi, "Exploring the full potentials of iot for better financial growth and stability: A comprehensive survey," *Sensors*, vol. 23, no. 19, 2023.

[12] C.-K. Wu, *Internet of Things Security, Architectures and Security Measures*. Springer Singapore, 1 ed., 05 June 2022.

[13] S. P. Khanna Rajesh, "Internet of things: Architectures, protocols, and applications," *Hindawi*, 2017.

[14] D. Pirker, T. Fischer, C. Lesjak, and C. Steger, "Global and secured uav authentication system based on hardware-security," August 2021.

[15] F. D. Qinghao Tang, "Internet of things security: Principles and practice," December 2021.

[16] G. Muhammad, F. Alshehri, F. Karray, A. E. Saddik, M. Alsulaiman, and T. H. Falk, "A comprehensive survey on multimodal medical signals fusion for smart healthcare systems," *Information Fusion*, vol. 76, pp. 355–375, 2021.

[17] I. Analytics, "Iot analytics: Market insights for the internet of things." `https://iot-analytics.com`, 2025. Accessed: 2025-01-11.

[18] R. Sindhuja, "A survey of internet of medical things (iomt) applications, architectures and challenges in smart healthcare systems," in *Proceedings of the International Conference on Data Science and Advanced Computing (ICDSAC)*, 2023.

[19] A. K. P. Sandeep Saxena, *Internet of Things- Security and Privacy in Cyberspace*. Singapore: Springer Singapore, 1 ed., 2022.

[20] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the internet of things," *Procedia Computer Science*, vol. 175, pp. 591–596, 2020. The 17th International Conference on Mobile Systems and Pervasive Computing (MobiSPC),The 15th International Conference on Future Networks and Communications (FNC),The 10th International Conference on Sustainable Energy Information Technology.

[21] A. I. Awad and J. Abawajy, *Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications*. 12 2021.

[22] D. Rani, N. Gill, and P. Gulia, "Classification of security issues and cyber attacks in layered internet of things," *Journal of Theoretical and Applied Information Technology*, vol. 100, 07 2022.

[23] I. Butun, *Industrial IoT Challenges, Design Principles, Applications, and Security: Challenges, Design Principles, Applications, and Security*. 01 2020.

[24] A. Alomari and S. A. Kumar, "Securing iot systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," *Internet of Things*, vol. 25, p. 101132, 2024.

[25] M. Bensalem, S. K. Singh, and A. Jukan, "On detecting and preventing jamming attacks with machine learning in optical networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2019.

[26] H. Boche, G. Janßen, and S. Kaltenstadler, "Entanglement-assisted classical capacities of compound and arbitrarily varying quantum channels," *Quantum Information Processing*, vol. 16, no. 4, pp. 1–31, 2017.

[27] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum iot networks," *Internet of Things*, vol. 9, 2020.

[28] A. Saritha, B. R. Reddy, and A. S. Babu, "Qemdd: Quantum inspired ensemble model to detect and mitigate ddos attacks at various layers of sdn architecture," *Wireless Personal Communications*, 2021.

[29] A. I. Awad and J. Abawajy, *Security and privacy in the Internet og things, architectures, techniques, and applications.* Wiley & Sons, 1 ed., December 2021.

[30] K. P. Anestis Papakotoulasa, Theodore Milonasb, *Improving IoT Security via Trusted Computing.* Social Science Research Network, 1 ed., June 27, 2023.

[31] T. Okediran, O. Vincent, A.-A. Adebayo, and J. Adeniran, "Securing the perceptual layer of the internet of things (iot) devices using elliptic curve cryptography," 04 2023.

[32] K. Manasa and L. M. I. Leo Joseph, *IoT Security Vulnerabilities and Defensive Measures in Industry 4.0*, pp. 71–112. Singapore: Springer Nature Singapore, 2023.

[33] Z. Zhou, P. Wang, and G. Li, "Bagua protocol: A whole-process configurable protocol for iot sensing devices security based on strong puf," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 805–819, 2024.

[34] A. Kama, M. Amar, S. Gaaton, K. Wang, Y. Tu, and Y. Oren, "Juliet-puf: Enhancing the security of iot-based sram-pufs using the remanence decay effect," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12715–12727, 2023.

[35] S. Alahmadi, H. Idriss, P. Rojas, and M. Bayoumi, "Security scalability of arbiter puf designs," *2023 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2023.

[36] X. Lu, "Implementation of art therapy assisted by the internet of medical things based on blockchain and fuzzy set theory," *Information Sciences*, vol. 632, pp. 776–790, 2023.

[37] C. Gonzalez-Amarillo, C. Cardenas-Garcia, M. Mendoza-Moreno, G. Ramirez-Gonzalez, and J. C. Corrales, "Blockchain-iot sensor (biots): A solution to iot-ecosystems security issues," *Sensors*, vol. 21, no. 13, 2021.

[38] H. Gehani and S. Rathkanthiwar, "A study on security of iot based blockchain system using artificial intelligence," pp. 1–6, 04 2023.

[39] "Research on security verification mechanism of perception layer terminal of power internet of things based on device operation fingerprint," vol. 692, no. 2, pp. 022024–, 2021.

[40] A. B. Price, J. G. Rarity, and C. Erven, "A quantum key distribution protocol for rapid denial of service detection," *EPJ Quantum Technology*, vol. 7, no. 1, 2020.

[41] F. Sabrina, S. Sohail, and U. U. Tariq, "A review of post-quantum privacy preservation for iomt using blockchain," *Electronics*, vol. 13, no. 15, 2024.

[42] R. P. Parameswarath and B. Sikdar, "Quantum-safe authentication protocol using post-quantum key encapsulation mechanism for transportation systems," pp. 1–6, 2024.

[43] N. N. Minhas, "Post-quantum authentication scheme for iot security in smart cities," 2024.

[44] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Z. Mussiraliyeva, and A. Chehri, "Pqcaie: Post quantum cryptographic authentication scheme for iot-based e-health systems," *Internet of things*, 2024.

[45] M. EI-Hadedy, P. V. Ankunda, J. Ung, and W.-M. Hwu, "Securing the internet of medical things (iomt) with k3s and hybrid cryptography: Integrating post-quantum approaches for enhanced embedded system security," in *2024 IEEE 17th Dallas Circuits and Systems Conference (DCAS)*, pp. 1–6, 2024.