JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Review Article

A Comprehensive Approach to Protocols and Security in Internet of Things Technology

Jean Pierre Ntayagabiri [1,*], Youssef Bentaleb [2], Jeremie Ndikumagenge [3], and Hind EL Makhtoum [2]

[1] Doctoral School of the University of Burundi, Center for Research in Infrastructure, Environment and Technology (CRIET), University of Burundi, Bujumbura, Burundi; e-mail : jpntayaga2@gmail.com
[2] Engineering Sciences Laboratory, ENSA Kenitra, Ibn Tofaïl University, Kenitra, Morocco; e-mail: ybentaleb@ymail.com; elmakhtoum_hind@live.fr
[3] Center for Research in Infrastructure, Environment and Technology (CRIET), University of Burundi, Bujumbura, Burundi; e-mail : jeremie.ndikumagenge@ub.edu.bi
* Corresponding Author: Jean Pierre Ntayagabiri

Abstract: The exponential growth of the Internet of Things (IoT) introduces a multitude of security challenges, as a vast number of connected devices often operate with inadequate protection measures. This vulnerability heightens the risk of cyberattacks, data breaches, and hacking, exposing systems and sensitive information to increased threats. Ensuring security in the IoT ecosystem while considering this rapidly expanding technology's physical limitations and specific requirements is a complex task. This article comprehensively analyzes the primary vulnerabilities and risks associated with IoT, exploring innovative strategies and effective solutions to strengthen its security framework. The article highlights the critical role of secure device authentication, data encryption, regular updates, and continuous monitoring by addressing the intricacies of communication protocols and emphasizing the need for standardization. Ultimately, this work advocates for a holistic approach to IoT security, where robust, adaptable solutions are developed to safeguard against the evolving landscape of cyber threats.

Keywords: Communication Protocols; Cybersecurity in IoT; Internet of Things (IoT) Security; Network Vulnerabilities; Secure Data Transmission.

1. Introduction

The rapid growth of the Internet of Things (IoT) technology has led to numerous advancements and opportunities in various sectors. From smart homes to industrial automation, IoT has revolutionized how we interact with our environment[1]. However, this expansion of IoT brings multiple security challenges[2]. With billions of devices exchanging data and communicating, vulnerabilities emerge that can be exploited by malicious actors[3], [4].

Recent reports underscore the critical importance of addressing these vulnerabilities. For instance, projections indicate that in 2025, there will be over 75 billion connected IoT devices, creating a massive attack surface[5]. Similarly, other reports highlight that IoT security breaches could cost organizations over $10 trillion annually due to data theft, service interruptions, and regulatory penalties[6]. This alarming trend emphasizes the need to systematically address IoT security and protocols to protect against rising threats.

The cybersecurity landscape for connected devices is complex and constantly evolving. Often poorly protected and heterogeneous, IoT devices are prime targets for cybercriminals[7]. They can be used to launch targeted or large-scale attacks, compromise user privacy, and disrupt critical infrastructures[7], [8]. For example, the Mirai botnet attack in 2016, which exploited IoT devices, demonstrated the catastrophic potential of unsecured devices, affecting essential services globally[9].

This article explores the importance of examining and improving protocols and security measures in IoT systems. Communication protocols such as Zigbee, Z-Wave, and LoRaWAN, which are critical to IoT systems, are often analyzed for their ability to ensure both reliability and security. According to an HP report, a deep understanding of these protocols

Received: October, 29th 2024
Revised: December, 8th 2024
Accepted: December, 13th 2024
Published: December, 24th 2024

and their vulnerabilities is essential, as studies reveal that 70% of IoT devices lack adequate security protections [10]. Bridging this gap is crucial for building a robust IoT ecosystem.

This scientific research aims to provide valuable insights into enhancing the protection of IoT systems against cyber threats. This study highlights the vulnerabilities malicious actors exploit by examining real-world use cases and analyzing existing security measures. It examines the potential consequences of a breach in an IoT ecosystem.

Moreover, this article explores key challenges such as device heterogeneity, lack of built-in security, weak passwords, lack of regular updates, large-scale attacks, lack of visibility and control, and insufficient legislative and regulatory frameworks. It also proposes potential solutions to mitigate these risks and evaluates emerging technologies and protocols designed to enhance IoT security.

This research aims to equip researchers and practitioners with a profound understanding of the challenges inherent to IoT security, enabling them to implement effective solutions and navigate the complexities of securing interconnected devices.

The rest of this article is organized as follows: Section 2 reviews related works on IoT communication protocols and security. Section 3 explores popular IoT communication protocols, highlighting their features and applications. Section 4 discusses the challenges encountered in the interconnected IoT ecosystem. Section 5 examines the security risks associated with the IoT. Section 6 synthesizes the challenges and corresponding security risks in IoT. Section 7 details various security techniques used to protect IoT systems. Section 8 presents a critical analysis of IoT communication protocols and security measures. Finally, Section 9 concludes the article.

2. Literature Review

The IoT has profoundly impacted our lives, connecting our homes, workplaces, and cities in ways once considered futuristic. However, this connectivity comes with its own set of security challenges that are imperative to address. A significant amount of research has been conducted on the topic of IoT security. Some key studies include:

- [11]–[13]: These papers provide an overview of IoT architecture, the protocols used at each layer, and common security issues.
- [14]–[16]: These studies focus on lightweight communication protocols and their security features, comparing options such as Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), and WebSocket.
- [17], [18]: These papers examine wireless communication techniques, IoT security technologies, and state-of-the-art methods for securing communications.
- [19]–[21]: These studies identify common attack types and vulnerabilities in IoT, analyzing risks in each layer and proposing mitigation solutions for specific applications like smart cities and Industry 4.0.
- [22], [23]: These papers broadly analyze IoT security challenges, reviewing existing research and proposing potential solutions.
- [24], [25]: These studies focus on security challenges in specific domains, such as healthcare and wireless sensor networks, proposing taxonomies of challenges and key technologies to address them.
- [26], [27]: These papers explore emerging approaches such as blockchain and software-defined networking to improve the flexibility and scalability of security and privacy in IoT.
- [28], [29]: These papers compare different IoT communication protocols based on their security features, energy consumption, and other functionalities.
- [30], [31]: These studies critically analyze existing IoT protocols and security research, identifying open challenges and research questions.

Despite substantial progress in IoT security, several critical gaps remain unaddressed. Existing studies often examine communication protocols or security measures independently, lacking an integrated approach that considers efficiency and security in complex IoT ecosystems. Additionally, the absence of universal standards for protocols and security practices has resulted in a fragmented landscape, limiting interoperability and complicating the implementation of cohesive solutions. Another significant gap lies in the insufficient exploration of security risks specific to large-scale infrastructures, such as smart cities and industrial systems,

where the implications of breaches can be catastrophic. Furthermore, while various mitigation techniques have been proposed, systematic comparative evaluations of their effectiveness across diverse IoT scenarios remain underexplored, leaving a need for a more comprehensive understanding of their practical applicability.

This review addresses these gaps by offering several key contributions. First, it provides a detailed comparative analysis of widely used IoT communication protocols, focusing on their security features and efficiency trade-offs to highlight their applicability in various contexts. Second, it identifies critical barriers and vulnerabilities in securing IoT ecosystems, particularly on large-scale and critical infrastructures, offering insights into these applications' unique challenges. Third, the review systematically evaluates existing security techniques, comparing their effectiveness in mitigating attacks across diverse IoT scenarios and identifying the most practical solutions. Finally, it proposes best practices and standardized guidelines to enhance IoT security, balancing the need for efficiency, scalability, and robust data protection, thereby contributing to a more resilient and interoperable IoT ecosystem.

3. Dive into Popular IoT Communication Protocols

Communication protocols play a fundamental role in the security of the IoT. They establish the rules and formats required for data exchange between IoT devices, servers, and other network components. Using secure communication protocols is essential to ensure data confidentiality, integrity, and availability in an IoT environment. These protocols must be designed to protect data against various threats, such as communication interception, malicious data tampering, replay attacks that reuse captured messages to im-personate legitimate devices, and denial-of-service (DoS) attacks aimed at overwhelming the network or rendering a device unavailable.

There are two main categories of communication protocols in IoT. The first concerns data communication protocols, which include standards such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Advanced Message Queuing Protocol (AMQP), Hypertext Transfer Protocol (HTTP), Extensible Messaging and Presence Protocol (XMPP), MQTT for Sensor Networks (MQTT-SN), and Data Distribution Service (DDS). These protocols primarily facilitate message transfer between devices and servers, considering the lightweight and efficient nature required in IoT environments.

The second category encompasses network communication protocols, such as Zigbee, Z-Wave, LoRaWAN, NB-IoT, Sigfox, Thread, Bluetooth Low Energy (BLE), Wi-Fi Direct, and cellular IoT standards like LTE-M and 5G NR-LTE IoT. These protocols focus more on managing physical connectivity and network infrastructure, offering solutions tailored to specific needs regarding range, power consumption, scalability, security, and interoperability with existing devices.

Understanding these protocols is crucial to designing robust IoT solutions that meet the specific requirements of different applications. Each protocol has strengths and weaknesses, which must be carefully evaluated to make informed decisions when implementing connected solutions. With this in mind, we propose an in-depth exploration of these protocols, starting with those dedicated to data communication.

3.1. Data Communication Protocols

3.1.1. Message Queuing Telemetry Transport (MQTT)

In the ever-evolving world of the IoT, reliable and efficient communication is the cornerstone of successful implementation. This is where the MQTT protocol, short for Message Queuing Telemetry Transport, comes into play, offering a game-changing solution.

MQTT is a lightweight messaging protocol designed explicitly for resource-constrained IoT devices unlike its bulkier counterparts. In the ever-evolving world of the IoT, reliable and efficient communication is the cornerstone of successful implementation. This is where the MQTT protocol, short for Message Queuing Telemetry Transport, comes into play, offering a game-changing solution[32]. It operates on top of the ubiquitous TCP/IP protocol, ensuring versatility and compatibility with diverse network infrastructures[33]. Its lightweight nature translates to minimal data usage, preserving the precious battery life of IoT devices [32].

MQTT leverages a publish-subscribe model. Devices can publish messages to specific topics, akin to channels, and subscribe to receive messages published to those topics[34]. This

decoupling between senders and receivers fosters scalable and flexible communication amongst numerous devices, eliminating the need for direct point-to-point connections.

Another notable feature is MQTT's support for Quality of Service (QoS) levels[35]. These levels dictate the reliability and delivery guarantees of messages exchanged between devices. MQTT provides three levels of QoS to manage message delivery, as illustrated in Figure 1. QoS 0, referred to as "at most once," offers no message delivery guarantee. Messages are not stored, and if delivery fails, they are lost. However, no duplication occurs in this mode since there is no retransmission. QoS 1, known as "at least once," ensures that the message is delivered at least once, even if this means retransmitting the message until an acknowledgment is received. This process may lead to duplicate receptions. Finally, QoS 2, or "exactly once," guarantees the delivery of messages precisely one time. This level of service employs a four-step handshake process (PUBLISH, PUBREC, PUBREL, PUBCOMP) to ensure the highest level of reliability, preventing both message loss and duplication.

This flexibility empowers developers to strike a balance between reliability and network bandwidth usage, selecting the most suitable QoS level for their specific needs. While boasting numerous advantages, MQTT inherently lacks built-in security features. While it supports encryption via Secure Sockets Layer (SSL) or TLS protocols, additional measures are necessary to guarantee end-to-end security in IoT deployments[36]. Additionally, scalability can become an obstacle in large-scale deployments involving thousands or millions of connected devices[37]. The surge in message traffic can potentially overload message brokers or consume excessive bandwidth if not managed effectively.

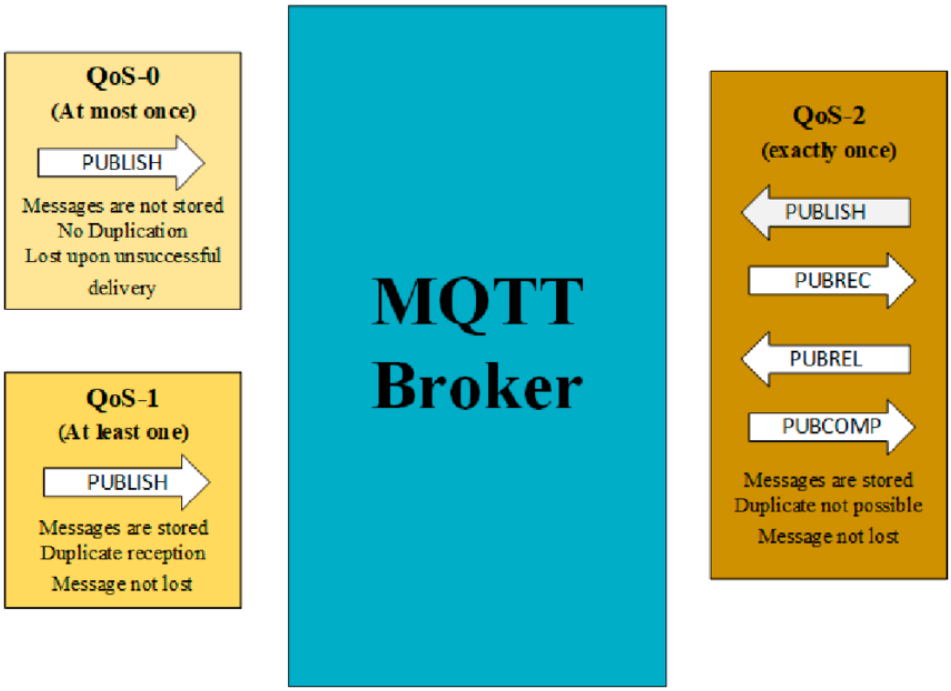

Figure 1. QoS-0-, QoS-1- and QoS-2-based MQTT broker with message delivery, duplication and storage status on the publishing node[38].

3.1.2. Hypertext Transfer Protocol (HTTP)

The HTTP protocol, a mainstay of web communication, is now emerging as a viable option for IoT applications[39]. This widely used protocol allows IoT devices to communicate with each other and with web servers, leveraging existing internet infrastructure[40].

One of the main advantages of using HTTP for IoT is its ability to leverage the existing infrastructure. By employing HTTP, IoT devices can benefit from the extensive web communication infrastructure already in place, reducing the need for additional development efforts[30]. Another advantage is its ease of use. HTTP's well-documented nature and widespread understanding make it developer-friendly, simplifying both implementation and trouble-shooting[40]. Furthermore, HTTP allows for seamless communication, as the standard ports (80 for unencrypted and 443 for encrypted connections) used by HTTP generally avoid

firewall restrictions when communicating with web servers[41]. This enables communication between diverse devices from various manufacturers, as long as they support HTTP, regardless of their specific operating system or hardware. HTTP thus acts as a common language, facilitating communication between different devices and fostering interoperability within an existing ecosystem.

However, there are also challenges associated with HTTP for IoT. One significant issue is data transfer efficiency. HTTP can be inefficient when dealing with small data sizes, as the protocol's headers, while crucial for communication, can be relatively large compared to the actual data being exchanged between devices [42]. This overhead can lead to increased bandwidth usage and potentially slower transmission speeds[38], [42]. Another challenge is security. While HTTP offers security measures like TLS encryption through HTTPS, it might not be suitable for highly sensitive data requiring more robust security protocols[4]. In such cases, additional security layers may be necessary on top of basic HTTPS to ensure adequate protection. Lastly, interoperability issues can arise when devices have varying levels of HTTP support or implement the protocol differently. This can lead to compatibility issues and require additional effort to ensure smooth communication between devices.

3.1.3. Constrained Application Protocol (CoAP)

The CoAP has been specifically designed to meet the unique requirements of resource-constrained devices commonly found in the IoT ecosystem, such as low-power sensors and actuators[5]. Its lightweight design minimizes resource consumption, making it particularly suitable for devices with limited processing power, memory, and battery life[43]. Compared to widely used protocols like MQTT and HTTP, CoAP distinguishes itself through its remarkable efficiency[5].

One of CoAP's greatest strengths lies in its resource-friendly nature. It is specifically tailored to prioritize minimal resource consumption, which is essential for devices with restricted power supply, processing capability, and memory[44]. CoAP is also recognized as an efficiency champion, offering superior performance compared to MQTT and HTTP in IoT environments[5]. Additionally, CoAP provides versatility by supporting both request/response interactions, similar to HTTP, and asynchronous messaging, like MQTT. This flexibility makes it a highly adaptable protocol for diverse IoT applications[45]. Another advantage is its reduced network overhead. By leveraging the UDP transport protocol, CoAP eliminates the need for permanent connections before data transfer, unlike TCP used by MQTT. This design reduces packet count and alleviates network congestion[43]. Furthermore, CoAP employs compact binary headers instead of HTTP's large request/response headers, improving bandwidth efficiency[45]. These characteristics make CoAP an excellent choice for constrained networks with limited bandwidth or intermittent connectivity[44]. CoAP's support for multicasting further enhances its efficiency by allowing devices to disseminate information simultaneously to multiple recipients within a network. This feature is particularly advantageous for applications such as environmental monitoring[46].

However, CoAP's benefits are accompanied by several challenges related to security. One major limitation is its lack of built-in security features, which makes it vulnerable to attacks such as eavesdropping, data alteration, and message replay[47]. Additional mechanisms like Datagram Transport Layer Security (DTLS) must be implemented on top of CoAP[48]. While DTLS provides necessary protection, it introduces complexity and overhead, potentially undermining CoAP's resource efficiency. Another drawback lies in CoAP's limited identity management. Its basic implementation lacks robust mechanisms for device authentication and authorization, which can create challenges in scenarios where secure access control and identification are critical[49]. External mechanisms such as certificates or preshared keys may need to be incorporated to address these shortcomings. Additionally, the overall security of CoAP deployments depends heavily on proper implementation. Vulnerabilities can arise due to misconfigurations or weaknesses specific to a given implementation, which may compromise the system's security posture[50].

3.1.4. Message Queuing Telemetry Transport for Sensor Networks (MQTT-SN)

In the realm of IoT communication, there are often comparisons between MQTT-SN and its parent protocol, MQTT. While MQTT has established itself as a popular and lightweight publish-subscribe protocol in the IoT domain, renowned for its simplicity, efficiency, and reliability[51], Message Queuing Telemetry Transport for Sensor Networks (MQTT-SN) offers a more specialized approach.

Designed specifically for constrained network environments prevalent in sensor networks, MQTT-SN addresses the unique challenges these resource-limited devices face [52]. It acts as an extension of MQTT, catering to the specific needs of sensor networks by introducing functionalities not present in the original protocol[33].

While both protocols share the objective of facilitating efficient communication within the IoT landscape, some key aspects set them apart. Notably, MQTT-SN:

- Expands Network Support: Overcomes limitations by supporting non-TCP/IP networks, whereas MQTT relies solely on TCP/IP connectivity[53].
- Enables Direct Communication: Eliminates the dependency on a central broker, allowing direct communication between sensors and gateways, making it suitable for scenarios with intermittent or unreliable network connectivity.

In contrast, MQTT operates through a central broker, making it more appropriate for environments with consistent TCP/IP availability[54]. It is crucial to acknowledge that neither MQTT nor MQTT-SN possess built-in security features, making them inherently vulnerable to various attacks like eavesdropping, data tampering, and message replay. To ensure secure communication in both protocols, additional security mechanisms, such as TLS or DTLS, need to be implemented on top of the core protocol functionality[55].

3.1.5. Extensible Messaging and Presence Protocol (XMPP)

In the world of IoT communication, XMPP and MQTT often surface in discussions. While both XMPP and MQTT facilitate communication within the IoT, their fundamental design and focus differ. Initially designed for instant messaging, XMPP has evolved into a contender in the IoT space. Its core strengths lie in its scalability, flexibility[56], and support for real-time communication facilitated by XML-based messages. XMPP devices can readily exchange various data types, control commands, and even presence information (e.g., online/offline status). In contrast, MQTT stands out as a lightweight publish/subscribe protocol explicitly designed to cater to the needs of resource-constrained IoT devices[57]. It ensures minimal overhead and efficient communication in environments where bandwidth, power, and processing capabilities are limited.

The choice between XMPP and MQTT often hinges on the specific requirements of your IoT application:

- Real-time Communication and Presence: If your application relies heavily on real-time interactions or the exchange of presence information, XMPP's strengths in these areas make it a suitable choice. Think of applications like smart home automation or collaborative work environments.
- Resource Constraints: When dealing with devices limited in power, memory, or bandwidth, MQTT's inherent efficiency and lightweight messaging format significantly reduce overhead.

It's crucial to acknowledge that neither protocol possesses robust built-in security mechanisms. Implementing additional security measures like TLS or suitable encryption methods is necessary to protect the integrity and confidentiality of data exchanged within XMPP or MQTT-based IoT systems.

3.1.6. Data Distribution Service (DDS)

In the realm of IoT real-time systems, the DDS has emerged as a powerful communication standard[58]. This protocol provides a robust framework for distributing data seamlessly among various devices, enabling real-time collaboration and communication[59].

One of the key strengths of DDS lies in its readiness for large-scale deployments. Unlike many other protocols, DDS excels in handling extensive networks involving thousands or even millions of interconnected devices[60]. Its publish-subscribe model further enhances efficiency in data distribution. In this model, publishers disseminate information exclusively to registered subscribers, minimizing unnecessary network traffic and ensuring timely data delivery [61]. Additionally, DDS incorporates advanced features such as QoS settings. These features allow developers to prioritize specific data types based on their criticality or urgency, ensuring that essential information receives immediate attention while less time-sensitive updates are processed appropriately[62]. Moreover, DDS stands out for its exceptional scalability and interoperability. It integrates seamlessly with existing systems, regardless of the programming languages or operating systems involved, making it an ideal choice for organizations operating within complex technological environments[63].

Despite its numerous advantages, DDS shares a common limitation with other messaging protocols: the lack of built-in security features. It is crucial to implement additional security measures, such as encryption and access control mechanisms to safeguard the confidentiality, integrity, and availability of data transmitted within DDS-based systems. These enhancements are essential for ensuring the secure operation of DDS in IoT ecosystems.

3.1.7 Summary

This section highlights the diverse communication protocols used in IoT ecosystems, each tailored to specific application needs and device constraints. Protocols like MQTT and CoAP are lightweight efficient, while HTTP and XMPP prioritize compatibility and real-time interactions. Advanced options like DDS address scalability in complex deployments, and MQTT-SN caters to constrained environments. Despite their strengths, the lack of built-in security across most protocols underscores the critical need for supplementary protective measures to ensure secure IoT operations. Selecting the right protocol requires careful consideration of use case requirements, resource limitations, and security needs.

3.2. Network Communication Protocols

3.2.1. Zigbee

Within the realm of IoT networks, the Zigbee protocol has carved a niche as a dependable and efficient solution for low-power devices[12]. It's defining characteristic lies in its mesh networking capabilities, fostering seamless connections between devices, making it a prime choice for home automation and industrial applications[12]. Zigbee's core design prioritizes communication between low-power devices, perfectly aligning with the needs of battery-powered sensors and actuators that demand extended operation without frequent battery replacements[44]. Leveraging a mesh network architecture, Zigbee empowers devices to communicate with each other via multiple paths, ensuring robust connectivity even in challenging environments[64]. This redundancy helps mitigate the impact of single points of failure, contributing to overall network reliability.

Zigbee boasts impressive scalability, supporting the operation of thousands of nodes within a single network[65]. This allows it to seamlessly adapt to complex systems without compromising performance or reliability. Zigbee prioritizes exceptional security measures, safeguarding data confidentiality and preventing unauthorized access. Its built-in AES-128 encryption provides end-to-end security, offering users peace of mind in today's interconnected world[43]. Furthermore, this protocol fosters interoperability, enabling seamless communication within the same network between devices from different brands and types, promoting a more unified and inclusive IoT environment.

3.2.2. Z-Wave

In the ever-evolving world of smart homes and the IoT, the Z-Wave protocol stands out as a reliable and secure communication solution[66]. Its foundation lies in low-power radio frequency operation, making it energy-efficient and perfectly suited for battery-powered devices commonly found in smart homes[67]. Z-Wave's inherent mesh networking capabilities empower devices to seamlessly communicate with each other, establishing a robust and reliable network within your smart home environment[68]. This decentralized approach ensures connectivity is maintained even if individual devices face challenges.

What truly sets Z-Wave apart is its exceptional compatibility with various manufacturers of smart devices [69]. This interoperability grants users the flexibility to choose from a diverse range of products while ensuring seamless integration into their existing smart home setup. No more limitations or frustrations due to incompatible systems. Z-Wave takes security very seriously, employing advanced encryption techniques to safeguard the data transmitted between your smart home devices[69]. This unwavering focus on security empowers you to trust your connected devices, knowing your privacy is protected and potential cyber threats are mitigated.

3.2.3. Long Range Wide Area Network (LoRaWAN)

The LoRaWAN distinguishes itself within the IoT eco-system by leveraging low data rates for long-distance transmission[70]. This unique approach enables devices to transmit data across several kilometers, making it particularly well-suited for large-scale deployments in diverse sectors. In smart cities, for instance, LoRaWAN facilitates connectivity for traffic

sensors, environmental monitoring systems, and smart lighting infra-structure across expansive urban areas. Similarly, industrial automation ensures efficient communication between industrial sensors, actuators, and control systems over vast factory premises or sprawling industrial complexes. In agriculture, LoRaWAN supports long-range monitoring of critical parameters such as soil moisture and temperature, even in remote lo-cations.

One of the key advantages of LoRaWAN is its exceptional range. It can penetrate dense urban environments and reach deep inside buildings, ensuring reliable connectivity even in challenging conditions[71]. This capability makes it a cost-effective alternative to the dense deployment of traditional network infrastructures. LoRaWAN devices are designed for minimal power consumption, resulting in extended battery life. Devices can operate for years on battery power without frequent replacements, which is particularly advantageous for deployments in remote or hard-to-reach locations, minimizing maintenance requirements[72]. Another notable strength of LoRaWAN is its impressive scalability. It can support thousands of devices within a single network while maintaining efficient communication and minimizing interference. It is ideal for large-scale deployments where numerous devices or sensors need to be connected and monitored simultaneously[73].

Despite its strengths, LoRaWAN does have some limitations. One of its primary drawbacks is its relatively low data rate compared to other wireless protocols such as Wi-Fi, NB-IoT, or cellular networks[74]. While this limitation is not a concern for applications that transmit small data packets infrequently (e.g., sensor readings), it may not be suitable for use cases requiring high-speed data transfer. LoRaWAN's reliance on unlicensed public radio frequencies also makes it vulnerable to congestion and interference from other devices or nearby networks operating on the same frequencies[75]. This susceptibility can potentially degrade the network's overall performance and reliability, particularly in densely populated areas.

3.2.4. Sigfox

Sigfox relies on a low-power wide-area network (LPWAN) architecture, enabling long-distance communication with exceptionally low energy consumption[76]. This makes it an excellent choice for connecting devices with limited power sources and low data rate requirements, such as sensors, trackers, and wearables.

One of Sigfox's main strengths is its extensive coverage, which ensures reliable connectivity even in remote or rural areas where traditional cellular networks or other protocols might struggle[77]. This makes it particularly well-suited for environmental monitoring, asset tracking, and remote infrastructure management applications. Additionally, as an LPWAN protocol, Sigfox emphasizes minimizing power consumption, resulting in extended battery life for connected devices. These devices can often operate for years on a single charge[78], a crucial advantage for deployments in isolated locations where frequent battery replacements are impractical. Moreover, Sigfox is characterized by its simplicity and cost-effectiveness. Its streamlined network architecture reduces complexity and associated costs, making it an attractive solution for projects requiring the connection of large numbers of devices.

Despite its advantages, Sigfox has some limitations. Its low data rate, a trade-off for reduced power consumption, makes it unsuitable for applications that demand real-time data transmission or large data transfers[78]. Furthermore, Sigfox primarily supports one-way communication, meaning devices can send data to the network but cannot directly receive information. While this is sufficient for some use cases, others may require two-way communication capabilities. Lastly, although Sigfox incorporates basic security measures, additional layers of security may be necessary depending on the specific requirements of the application.

3.2.5. Thread

Thread emerges as an open, low-power wireless networking protocol designed specifically to cater to the needs of IoT devices within the smart home environment[78]. Its core strengths lie in providing reliable and secure communication, making it a perfect choice for seamless interaction between numerous devices within a smart home ecosystem.

Thread leverages a mesh network topology, empowering devices to communicate directly with each other or via neighboring nodes[79]. This decentralized approach fosters robust connectivity throughout a home or building, ensuring continued operation even if individual devices encounter challenges. Thread excels in scalability, effortlessly supporting a large number of devices within a single network without compromising performance[78]. This inherent scalability makes it well-suited for even the most complex smart home setups, seamlessly integrating numerous sensors, actuators, and other IoT devices.

Thread prioritizes security, safeguarding data transmission within the network. It employs robust encryption techniques and authentication mechanisms, guaranteeing that only authorized devices can access and communicate with each other[80]. This focus on security provides peace of mind, knowing your smart home network is protected from unauthorized access. Thread's compatibility with IPv6 facilitates seamless integration with existing IP networks, promoting interoperability between diverse IoT platforms and ecosystems[78]. This flexibility makes it an attractive option for manufacturers seeking to develop interconnected smart home solutions that can effortlessly communicate with other IoT devices, regardless of brand or platform.

3.2.6. Summary

This section underscores the diverse landscape of network communication protocols available for IoT applications, each tailored to meet specific requirements. Zigbee and Z-Wave excel in low-power, secure communication for smart homes and automation, while LoRaWAN and Sigfox cater to long-range, low-power use cases in remote or large-scale deployments. Thread offers scalable, IPv6-compatible solutions for seamless integration in smart homes. Despite their unique advantages, challenges like limited data rates, interoperability, and security considerations highlight the importance of selecting the proper protocol based on specific application needs and constraints.

4. Discover The Challenges of The Interconnected World

The IoT envisions a seamless integration of intelligent devices into everyday life, offering unprecedented convenience and efficiency. However, achieving this vision entails navigating a complex web of challenges. These obstacles span the security vulnerabilities of devices, the limitations of existing network infrastructures, and the risks associated with data management. Addressing these challenges is essential to unlock the full potential of IoT while ensuring safety and reliability.

4.1. The Hydra of Vulnerability

The diversity of IoT devices presents a multifaceted challenge. These devices range from resource-constrained sensors to sophisticated smart gadgets, each requiring unique security solutions tailored to their specific capabilities[81]. Legacy systems further complicate this landscape; many older devices lack integrated security features, creating vulnerabilities in otherwise secure networks[8]. Modernizing or replacing these systems is often expensive and technically demanding. Another critical issue is the physical accessibility of IoT devices. Many, such as cameras, sensors, and smart meters, are prone to tampering. This can expose sensitive data or disrupt their intended functionality, posing significant risks to security and privacy.

4.2. The Network Storm

IoT's reliance on diverse connectivity protocols and communication technologies creates a fragmented network landscape. This lack of standardization leads to compatibility challenges and undermines secure communication between devices from different manufacturers [4], [82]. Additionally, the decentralized nature of IoT networks complicates efforts to implement unified security measures, leaving gaps that malicious actors can exploit[83]. As the number of connected devices grows exponentially, existing network infrastructures face mounting pressure to scale effectively. Ensuring robust and secure management of this vast network is a formidable challenge that requires innovative solutions[5].

4.3. The Charybdis of Data

IoT generates an overwhelming volume of data, straining the capacity of current processing and storage systems. Securing this data while maintaining efficient operations and protecting user privacy is a delicate balancing act[84]. Privacy concerns are particularly acute, as IoT systems must find ways to collect and utilize valuable data without compromising transparency or user control. Striking this balance requires thoughtful policies and responsible data processing practices. The interconnected nature of IoT further exacerbates security risks. A single breach can cascade across devices and networks, exposing sensitive information on a massive scale[85].

Despite these challenges, the future of IoT remains promising. A secure and thriving IoT ecosystem can be created by embracing innovation, fostering collaboration, and addressing these barriers. Establishing standardized communication protocols and ensuring device

interoperability will enhance secure and efficient data exchange. Adopting a "security by design" approach, where robust security measures are integrated at both the device and network levels from the outset, will minimize vulnerabilities. Leveraging advanced threat detection tools powered by machine learning and AI will enable real-time responses to emerging cyber threats. Lastly, fostering user education and awareness will empower individuals to adopt responsible data-sharing practices, strengthen privacy settings, and promote a security culture in this interconnected world.

5. An In-Depth Look at The Security Risks of The Internet of Things

The IoT represents a technological marvel, intricately weaving connectivity into the fabric of daily life. However, this interconnected ecosystem also brings with it a plethora of security challenges. Each IoT device connected to a network serves as a potential entry point for hackers, collectively expanding what is known as the "attack surface"—the total number of avenues for unauthorized access to a system, including devices, network connections, and software[86], [87]. IoT security threats are typically categorized into three broad areas: exploits like remote code execution and command injection, malware such as botnets and Trojans, and user-related vulnerabilities, including weak passwords and phishing attacks[88]. Understanding the vulnerabilities at every layer of the IoT ecosystem is critical to combating these threats.

At the device level, vulnerabilities often arise from outdated or insecure firmware. Hackers can exploit these flaws to gain unauthorized control over devices, compromising their functionality and integrity. Physical tampering is another significant risk; attackers with access to IoT devices can extract sensitive data or embed malicious hardware. Furthermore, weak crypto-graphic implementations, such as inadequate encryption algorithms or poor key management practices, expose sensitive data like passwords or sensor readings to attackers. Ensuring robust device-level security is the first line of defense in protecting IoT ecosystems.

Unsecured communication channels present a major threat at the network level. Unencrypted data transmissions are particularly vulnerable to interception, exposing sensitive user information and device controls. Compromised devices are often recruited into botnets—large-scale networks of infected devices—used to execute distributed denial of service (DDoS) attacks that can disrupt critical infrastructure or services. Additionally, attackers can exploit vulnerabilities in a single device to move laterally within the network, gaining access to other interconnected systems. Effective network security measures are essential to mitigate these risks and safeguard IoT infrastructures.

At the data level, IoT systems are susceptible to breaches that target sensitive information such as personal or financial data. Unregulated data collection practices often lead to privacy intrusions, while the misuse of IoT-collected data can result in malicious activities like targeted advertising or manipulating public opinion. Securing IoT-generated data requires comprehensive policies and practices that ensure data privacy, proper handling, and transparency in its use.

Achieving IoT security demands a multi-layered approach that addresses vulnerabilities across devices, communication protocols, and data management while fostering user awareness[89]. Despite notable advancements in IoT technology, significant gaps persist. Studies reveal that 57% of IoT devices are exposed to medium or high-severity vulnerabilities, making them attractive targets for cybercriminals[90], [91]. Once compromised, a device can serve as a gateway for attackers to infiltrate other systems within the network. Exploits, as depicted in Figure 2, are among the most prevalent threats, employing malicious code to disrupt systems or steal data. While these attack techniques are generally outdated by modern cybersecurity standards, their simplicity remains effective against IoT devices.

This vulnerability stems from several factors, including a lack of security by design in many IoT devices, reliance on outdated or insecure software and firmware, and challenges in applying security patches due to the limited computing power and intermittent connectivity of IoT devices. Additionally, many users are unaware of the risks associated with IoT and fail to adopt best practices to secure their devices. Addressing these issues requires a holistic effort to integrate robust security measures into IoT devices, streamline updates, and promote user education to build a more secure IoT ecosystem.

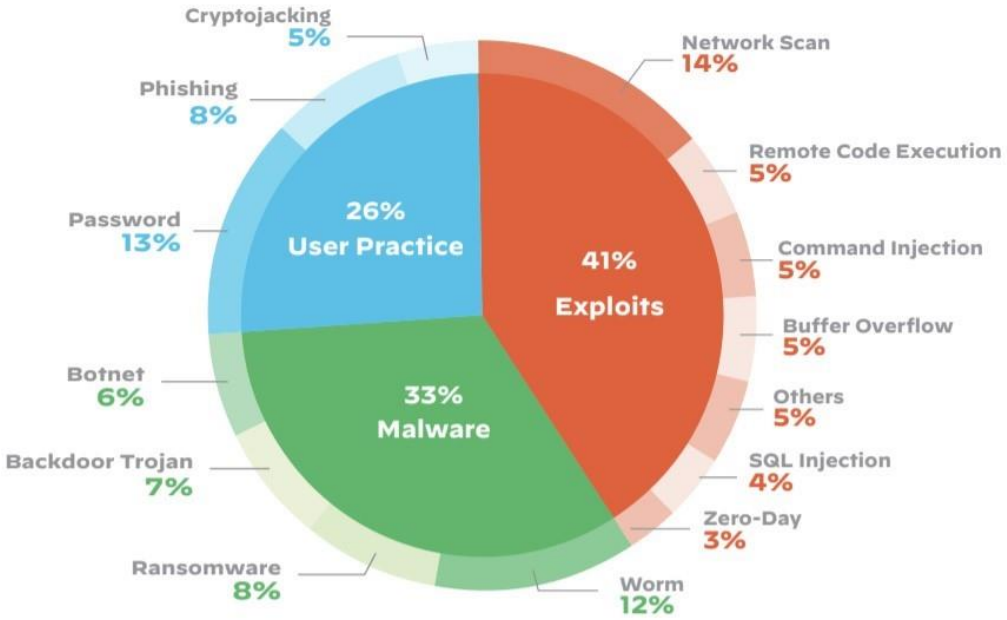

Figure 2. Summary of Top IoT Threats by Category [91]

6. Synthesis of Challenges and Associated Security Risks for The IoT

The IoT is disrupting our world by connecting a myriad of devices and transforming our daily interactions. This revolution brings with it a multitude of opportunities for businesses and individuals, but it also raises new challenges and security concerns, as illustrated in the previous sections. Drawing on Table 1, this section will synthesize IoT's major challenges and the associated security risks.

Table 1. IoT Challenges and Security Risks.

Challenge	Description	Security Risks
Diversity of Protocols	Numerous protocols exist for different applications, creating a fragmented landscape[18].	Difficulty in securing a diverse landscape, vulnerabilities easily spread across protocols.
Lack of Standardization	No universal standards for protocols and security practices exist.	Increased complexity, security fragmentation, and interoperability issues.
Limited Resources	Many IoT devices have low processing power and memory[92].	Difficulty implementing robust security solutions, resource-intensive encryption, and complex updates.
Unsecured Devices by Design	Many devices lack built-in security features, prioritizing cost and functionality [82].	Vulnerable to attacks, easy access for unauthorized users.
Outdated Software and Firmware	Difficulty updating software and firmware due to limited resources and connectivity [93].	Unpatched vulnerabilities, exposed to known exploits.
Weak Authentication and Authorization	Inadequate user authentication and authorization practices[82], [94].	Unauthorized access, data manipulation, and identity theft.
Lack of User Awareness	Many users are unaware of IoT security risks and best practices[95].	Unintentional security vulnerabilities, susceptibility to social engineering attacks.
Insecure Network Connections	Insecure network connections (e.g., unencrypted Wi-Fi) expose data to eavesdropping or manipulation.	Data breaches, privacy violations, compromised device control.
Physical Insecurity	Some devices are physically vulnerable to tampering or theft[96].	Data breaches, device hijacking, and potential physical harm if connected to critical infrastructure.

7. Understanding Key IOT Security Strategies

The IoT revolutionizes how devices interact, but this interconnected ecosystem also exposes significant security vulnerabilities. IoT security aims to address these risks through strategies such as detachable networks, access restrictions, and behavior monitoring, which protect against threats ranging from data breaches to malware. However, the rush to dominate the IoT market has led many vendors to prioritize low-cost solutions at the expense of robust cybersecurity. Many devices are released without ongoing software updates or security patches, exposing them to attacks. Table 2 highlights some IoT devices with the most notable security flaws. Unsecured networks further exacerbate this issue, as 98% of IoT device communications occur without encryption[94]. Such vulnerabilities enable attackers to intercept sensitive information, often exploiting it for profit on the dark web. As IoT devices become more pervasive, moving beyond basic safeguards and adopting a more comprehensive security approach is essential.

At the device level, robust hardware and software measures are vital for safeguarding IoT systems. Hardware Security Modules (HSMs), tamper-resistant chips that store cryptographic keys, ensure secure operations even if the device is compromised. Secure boot mechanisms verify the integrity of firmware during startup, allowing only legitimate software to run. Secure coding practices further minimize exploitable flaws by adhering to rigorous standards and conducting vulnerability assessments. Additionally, over-the-air firmware updates enhance resilience by addressing vulnerabilities quickly and efficiently.

Table 2. IoT Devices with the Highest Share of Security Issues.

IoT devices	Share security concerns
Medical Imaging Systems	51%
Security cameras	33%
Patient Monitoring Systems	26%
Printers	24%
Medical device gateways	9%
Consumer electronics	7%
Energy management devices	6%
IP Phones	5%

The network layer also plays a crucial role in ensuring IoT security. Zero Trust Network architectures, built on the principle of "never trust, always verify," require devices and users to authenticate themselves continually. Microsegmentation, which divides networks into isolated segments, limits attackers' ability to move laterally within the system. Threat intelligence and intrusion detection systems (IDS/IPS) enable real-time network traffic monitoring, helping to identify and neutralize suspicious activity. Encrypted communication protocols such as TLS/SSL and WPA3 further protect data in transit, ensuring it cannot be intercepted or tampered with.

Data security is equally important in protecting sensitive information generated by IoT devices. Differential privacy introduces controlled noise into datasets during collection, preserving statistical utility while safeguarding individual privacy. Homomorphic encryption allows computations to be performed on encrypted data without requiring decryption, ensuring sensitive information remains secure throughout processing. Secure Multi-Party Computing (MPC) enables collaborative analysis across multiple entities while maintaining data confidentiality. Data provenance and tracking ensure traceability, building trust and accountability in data management processes.

Finally, the application level demands rigorous protection to ensure the integrity of IoT systems. Robust API security measures, including authentication and rate limit, prevent unauthorized access and abuse. Regular penetration testing and vulnerability assessments proactively identify and address weaknesses before attackers can exploit them. Enforcing secure coding practices and utilizing open-source security tools help minimize application vulnerabilities. Sandboxing and execution analysis isolate untrusted applications, enabling real-time detection of potentially malicious behavior.

Securing IoT requires a multi-layered approach that addresses vulnerabilities across all levels. Continuous research and development are crucial to countering evolving threats and ensuring the safety of the interconnected IoT ecosystem. Table 3 provides a comparative analysis of popular IoT security techniques, emphasizing the need for layered defenses to protect this vast and complex landscape.

Table 3. Internet of Things Security Techniques.

Technique	Description	Strengths	Weaknesses	Typical Applications
Authentication and Authorization	Verifying device identity and access rights.	Granular control over access prevents unauthorized access.	It can be complex to implement and requires secure storage for credentials.	All IoT devices and systems
Data Encryption	Protecting data in transit and at rest.	Confidentiality protects sensitive information and prevents data breaches.	It can impact performance on resource-constrained devices and requires key management.	Data transmission, storage, and IoT ecosystem
Secure Boot	Verifies device firmware integrity before boot.	Prevents unauthorized firmware tampering and ensures the device runs legitimate software.	Requires specialized hardware and software support, which may not be feasible for all devices.	Critical system components, boot processes
Patch Management	Timely updates to address vulnerabilities.	Mitigates known security flaws, improves overall system resilience.	It can be challenging for large deployments, requires secure update mechanisms.	All software components and IoT infrastructure firmware
Network Segmentation	Isolating different parts of the network.	Limits the spread of security breaches, protects critical systems from compromised devices.	Increases network complexity, requires careful configuration and monitoring.	Industrial control systems, medical devices, infrastructure
Identity and Access Management (IAM)	Centralized management of user and device identities.	Simplifies access control, provides audit trails for activity tracking.	It can be complex for large deployments, requires secure and reliable infrastructure.	Cloud-based IoT platforms, enterprise deployments
Secure Sockets Layer (SSL/TLS)	Encrypting communication channels.	Protects data in transit, provides secure communication channels.	It can impact performance on resource-constrained devices and requires certificate management.	Web-based communication, device-to-cloud interactions
Intrusion Detection and Prevention Systems (IDS/IPS)	Monitoring network traffic for suspicious activity.	Detects and blocks potential attacks, proactively identifies anomalous behavior.	It can generate false positives and may require specialized expertise for configuration and analysis.	Network gateways, critical infrastructure protection
Firmware Signing and Verification	Ensuring firmware authenticity and integrity.	Prevents unauthorized firmware installations, and verifies software integrity before deployment.	Requires secure signing keys and infrastructure, which may not be feasible for all devices.	Firmware updates, boot processes, embedded systems
Secure Coding Practices	Implementing secure coding principles to avoid vulnerabilities.	Reduces software vulnerabilities, a proactive approach to security flaws.	Requires developer training and awareness, which can be time-consuming and resource-intensive.	All software development stages for IoT systems

8. Critical Analysis of Internet of Things Communication Protocols and Security Techniques

Communication protocols are a crucial element of the IoT. Their diverse nature allows them to meet the specific needs of each application, and their continuous improvement aims to bolster security. However, the lack of a universal standard and the implementation complexity pose significant challenges.

Security vulnerabilities in communication protocols expose IoT devices to various threats that hackers can exploit to access devices and data. Brute force attacks, replay attacks, DoS attacks, and code injection attacks are just a few examples of the dangers faced by IoT. The consequences of these attacks can be severe, ranging from data theft to device control and service disruption.

Fortunately, several steps can be taken to minimize these risks. Data encryption, authentication, and authorization, regular software updates, network segmentation, suspicious activity monitoring and analysis, etc., are essential best practices for IoT security. However, these techniques also have their limitations and challenges.

Authentication and authorization, intended to guarantee controlled access to devices and data, have limitations in their current implementation for IoT. Vulnerabilities to dictionary attacks, phishing, brute force attacks, replay attacks, and other techniques threaten system security. Additionally, managing identities and access for a large number of IoT devices presents a significant challenge, highlighting the need for more robust and adaptable solutions.

Data encryption, a crucial element for protecting the confidentiality and integrity of sensitive data, faces challenges due to the limited resources of IoT devices. The diversity of architectures and operating systems complicates the implementation of compatible encryption solutions and raises concerns regarding efficient encryption key management. Therefore, developing lightweight and efficient encryption solutions becomes crucial for IoT security.

Implementing Secure Boot, which guarantees the integrity of the code executed at device startup, is complex for resource-constrained IoT devices. The lack of universal standards in this area hinders the widespread adoption of this promising technique and presents a fragmented security landscape.

Patch Management, designed to keep IoT devices up to-date with the latest security patches, faces challenges due to their intermittent connectivity and limited resources. The speed of response to discovered vulnerabilities becomes crucial to limit the risk of exploitation by hackers.

Network segmentation, a promising technique for limiting the impact of an attack to a single segment, suffers from the absence of universal standards. Implementing effective and interoperable segmentation solutions is essential for strengthening IoT security.

Identity and Access Management (IAM), which allows for precise access permissions to be defined for each IoT device, faces the complexity of managing identities and access for a large number of devices. The lack of universal standards in this area fragments security and limits the interoperability of solutions.

Intrusion Detection and Prevention Systems (IDS/IPS), while valuable for detecting suspicious activity on the IoT network, often generate false alarms for legitimate activities, undermining their effectiveness. Additionally, their ability to detect attacks targeting IoT devices requires further improvement, highlighting the need for continued adaptation and optimization of these systems.

Secure Sockets Layer (SSL/TLS), which encrypts data in transit between IoT devices and servers, can negatively impact network performance, especially for low-power devices. Finding a balance between security and performance is crucial for ensuring a smooth and optimal user experience.

Firmware signing and verification, techniques aimed at ensuring the authenticity and integrity of IoT device firmware, have limitations. The risk of compromised signing keys poses a major threat, and the lack of universal standards hinders the widespread adoption of this promising approach. Additionally, the diversity of architectures and operating systems complicates the implementation of interoperable signing and verification solutions.

This analysis of current security techniques for IoT reveals significant challenges and limitations. The diversity of protocols, limitations of authentication and authorization, challenges with encryption and Secure Boot, complexities of Patch Management and network segmentation, limitations of IAM, capabilities of IDS/IPS, performance impact of SSL/TLS, and vulnerabilities in firmware signing and verification highlight the need for a new, adaptable approach to ensuring IoT security.

9. Conclusions

The rapid development of the IoT has significantly transformed daily life, creating unparalleled opportunities for businesses and individuals. However, this technological revolution also introduces complex challenges, particularly concerning communication protocols and security.

Communication protocols are the backbone of IoT, facilitating the connection and data exchange between devices. While their diversity caters to the specific needs of various appli-

cations, it also leads to fragmentation, exacerbating security vulnerabilities. These vulnerabilities are further compounded by threats such as unauthorized access, data manipulation, theft of sensitive information, and ransomware attacks.

This research has achieved several objectives. It conducted a comparative analysis of IoT communication protocols, highlighting their strengths and weaknesses based on security, energy consumption, scalability, and interoperability criteria. It also identified IoT systems' primary challenges and vulnerabilities, emphasizing critical issues such as device heterogeneity, the absence of universal standards, and insufficient built-in security measures. Furthermore, the study proposed solutions and best practices to enhance the security of IoT devices and networks while maintaining a balance between efficiency, scalability, and data protection.

The findings of this research emphasize the need for a comprehensive and proactive approach to securing the IoT ecosystem. Crucial elements of this approach include robust device authentication paired with advanced encryption techniques, regular software updates, and continuous system monitoring to detect and mitigate threats. Standardizing protocols and security techniques is also vital to ensure interoperability and provide enhanced protection for large-scale connected infrastructures.

Despite these efforts, the study reveals that current measures remain inadequate. The limitations of existing protocols, coupled with threats' rapid evolution, demand ongoing security solutions advancements. Addressing these challenges necessitates fostering innovation, particularly by integrating emerging technologies such as artificial intelligence, machine learning, and big data analytics.

In conclusion, this study contributes to bridging gaps identified in the existing literature by providing a solid foundation for developing standardized practices and tailored security solutions. The ultimate goal is to build a secure, resilient, and sustainable IoT ecosystem where connected devices can operate confidently and reliably.

Author Contributions: Conceptualization: Jean Pierre Ntayagabiri; methodology, Jean Pierre Ntayagabiri and Hind El Makhtoum; software: Jean Pierre Ntayagabiri.; validation: Jean Pierre Ntayagabiri, Hind El Makhtoum, Youssef Bentaleb and Jeremie Ndikumagenge; formal analysis: Jean Pierre Ntayagabiri; investigation: Jean Pierre Ntayagabiri and Hind El Makhtoum.; writing—original draft preparation: Jean Pierre Ntayagabiri.; writing—review and editing: Jean Pierre Ntayagabiri.; supervision: Youssef Bentaleb and Jeremie Ndikumagenge.

Funding: This research received no external funding.

Conflicts of Interest: There are no conflicts of interest.

References

[1] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *J. Big Data*, vol. 6, no. 1, p. 111, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[2] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *J. Clean. Prod.*, vol. 274, p. 122877, Nov. 2020, doi: 10.1016/j.jclepro.2020.122877.

[3] B. I. Mukhtar, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "IoT Vulnerabilities and Attacks: SILEX Malware Case Study," *Symmetry (Basel).*, vol. 15, no. 11, p. 1978, Oct. 2023, doi: 10.3390/sym15111978.

[4] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.

[5] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," *Comput. Sci. Rev.*, vol. 44, p. 100467, May 2022, doi: 10.1016/j.cosrev.2022.100467.

[6] E. H. Park, "Impact of Data Breaches on Different Sectors over Time: Stock Market Reaction," Capitol Technology University, 2024. [Online]. Available: https://search.proquest.com/openview/01a71a19e0925f784746b3b1a2c83878/1?pq-origsite=gscholar&cbl=18750&diss=y

[7] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, Aug. 2022, doi: 10.1016/j.iot.2022.100564.

[8] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 280–308, 2023, doi: 10.1016/j.iotcps.2023.04.002.

[9] B. Sutheekshan, S. Basheer, G. Thangavel, and O. P. Sharma, "Evolution of Malware Targeting IoT Devices and Botnet formation," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, Feb. 2024, vol. 5, pp. 1415–1422. doi: 10.1109/IC2PCT60090.2024.10486705.

[10] N. S. S, D. M. Anna, V. M N, and S. R. Kota, "Enabling Lightweight Device Authentication in Message Queuing Telemetry Transport Protocol," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 15792–15807, May 2024, doi: 10.1109/JIOT.2024.3349394.
[11] M. Ahmid and O. Kazar, "A Comprehensive Review of the Internet of Things Security," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, Jul. 2023, doi: 10.1080/19361610.2021.1962677.
[12] S. Choudhary and G. Meena, "Internet of Things: Protocols, Applications and Security Issues," *Procedia Comput. Sci.*, vol. 215, pp. 274–288, Dec. 2022, doi: 10.1016/j.procs.2022.12.030.
[13] P. Sharma, M. Kherajani, D. Jain, and D. Patel, "A Study of Routing Protocols, Security Issues and Attacks in Network Layer of Internet of Things Framework," in *2nd International Conference on Data, Engineering and Applications (IDEA)*, Feb. 2020, pp. 1–6. doi: 10.1109/IDEA49133.2020.9170741.
[14] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digit. Commun. Networks*, vol. 8, no. 6, pp. 1094–1104, Dec. 2022, doi: 10.1016/j.dcan.2022.03.013.
[15] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, vol. 14, p. 100129, Jun. 2021, doi: 10.1016/j.iot.2019.100129.
[16] A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Analysis on functionalities and security features of Internet of Things related protocols," *Wirel. Networks*, vol. 28, no. 7, pp. 2857–2887, Oct. 2022, doi: 10.1007/s11276-022-02999-7.
[17] N. A. Khan, A. Awang, and S. A. A. Karim, "Security in Internet of Things: A Review," *IEEE Access*, vol. 10, pp. 104649–104670, Dec. 2022, doi: 10.1109/ACCESS.2022.3209355.
[18] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, no. 1, pp. 1–25, Dec. 2017, doi: 10.1155/2017/9324035.
[19] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security Considerations for Internet of Things: A Survey," *SN Comput. Sci.*, vol. 1, no. 4, p. 193, Dec. 2020, doi: 10.1007/s42979-020-00201-3.
[20] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," *Sensors*, vol. 22, no. 19, p. 7433, Sep. 2022, doi: 10.3390/s22197433.
[21] R. Sharma and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 11, p. e4571, Nov. 2023, doi: 10.1002/ett.4571.
[22] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: a survey," *SN Appl. Sci.*, vol. 3, no. 1, p. 121, Jan. 2021, doi: 10.1007/s42452-021-04156-9.
[23] A. K. Abed and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," *Secur. Priv.*, vol. 6, no. 3, p. e285, May 2023, doi: 10.1002/spy2.285.
[24] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021, doi: 10.1109/JIOT.2021.3062630.
[25] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, p. e4946, Nov. 2020, doi: 10.1002/cpe.4946.
[26] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Comput. Networks*, vol. 141, pp. 199–221, Aug. 2018, doi: 10.1016/j.comnet.2018.03.012.
[27] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023, doi: 10.3390/s23020788.
[28] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, May 2017, pp. 685–690. doi: 10.1109/ICITECH.2017.8079928.
[29] C. Mahmoud and S. Aouag, "Security for Internet of Things," in *Proceedings of the 9th International Conference on Information Systems and Technologies*, Mar. 2019, pp. 1–6. doi: 10.1145/3361570.3361622.
[30] A. Zamfiroiu *et al.*, "IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data," *Proc. Int. Conf. Bus. Excell.*, vol. 14, no. 1, pp. 1109–1120, Jul. 2020, doi: 10.2478/picbe-2020-0104.
[31] P. Manna and R. K. Das, "Scalability in internet of things: Techniques, challenges and solutions," *Int. J. Res. Eng. Appl. Manag.*, vol. 7, no. 01, pp. 2454–9150, 2021, doi: 10.35291/2454-9150.2021.0175.
[32] K. P. Satamraju and M. B, "Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare," *Sensors*, vol. 20, no. 5, p. 1389, Mar. 2020, doi: 10.3390/s20051389.
[33] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S — A publish/subscribe protocol for Wireless Sensor Networks," in *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08)*, Jan. 2008, pp. 791–798. doi: 10.1109/COMSWA.2008.4554519.
[34] H. C. Hwang, J. Park, and J. G. Shon, "Design and Implementation of a Reliable Message Transmission System Based on MQTT Protocol in IoT," *Wirel. Pers. Commun.*, vol. 91, no. 4, pp. 1765–1777, Dec. 2016, doi: 10.1007/s11277-016-3398-2.
[35] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, Apr. 2015, pp. 746–751. doi: 10.1109/CSNT.2015.16.
[36] M. A. Spohn, "On MQTT Scalability in the Internet of Things: Issues, Solutions, and Future Directions," *J. Electron. Electr. Eng.*, p. 4, Oct. 2022, doi: 10.37256/jeee.1120221687.
[37] J. Ali, M. H. Zafar, C. Hewage, R. Hassan, and R. Asif, "Mathematical Modeling and Validation of Retransmission-Based Mutant MQTT for Improving Quality of Service in Developing Smart Cities," *Sensors*, vol. 22, no. 24, p. 9751, Dec. 2022, doi: 10.3390/s22249751.
[38] T. Yokotani and Y. Sasaki, "Comparison with HTTP and MQTT on required network resources for IoT," in *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, Sep. 2016, pp. 1–6. doi: 10.1109/ICCEREC.2016.7814989.

[39] Y. M. Algani *et al.*, "Integration of Internet Protocol and Embedded System On IoT Device Automation," *Research Square*. Dec. 17, 2021. doi: 10.21203/rs.3.rs-947704/v1.
[40] D. Gourley and B. Totty, *HTTP: the definitive guide*. " O'Reilly Media, Inc.," 2002. [Online]. Available: https://books.google.com/books?hl=fr&lr=&id=3EybAgAAQBAJ&oi=fnd&pg=PR5&dq=D.+Gourley+and+B.+Totty,+HTTP:+the+definitive+guide.++O'Reilly+Media,+Inc.,+2002.+Accessed:+Oct.+26,+2024.+%255BOnline%255D.+Available:+https://books.google.com/books%253Fhl%253Dfr%2526lr%253D%25
[41] W. M. Shbair, T. Cholez, J. Francois, and I. Chrisment, "A Survey of HTTPS Traffic and Services Identification Approaches," *arXiv*. arXiv, Aug. 19, 2020. [Online]. Available: http://arxiv.org/abs/2008.08339
[42] B. Wukkadada, K. Wankhede, R. Nambiar, and A. Nair, "Comparison with HTTP and MQTT In Internet of Things (IoT)," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Jul. 2018, pp. 249–253. doi: 10.1109/ICIRCA.2018.8597401.
[43] M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov, and M. Derawi, "A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 101362–101384, Dec. 2022, doi: 10.1109/ACCESS.2022.3207472.
[44] L. Duong, "The techniques of IoT and it's applications for smart homes: internet of things techniques and standards for building smart homes," 2023. [Online]. Available: https://lutpub.lut.fi/handle/10024/165971
[45] I. Ishaq, J. Hoebeke, F. Van den Abeele, J. Rossey, I. Moerman, and P. Demeester, "Flexible Unicast-Based Group Communication for CoAP-Enabled Devices," *Sensors*, vol. 14, no. 6, pp. 9833–9877, Jun. 2014, doi: 10.3390/s140609833.
[46] I. Ishaq, J. Hoebeke, I. Moerman, and P. Demeester, "Experimental Evaluation of Unicast and Multicast CoAP Group Communication," *Sensors*, vol. 16, no. 7, p. 1137, Jul. 2016, doi: 10.3390/s16071137.
[47] S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Mar. 2019, pp. 655–660. doi: 10.1109/ICACCS.2019.8728533.
[48] P. M. Kumar and U. D. Gandhi, "Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application," *J. Supercomput.*, vol. 76, no. 6, pp. 3963–3983, Jun. 2020, doi: 10.1007/s11227-017-2169-5.
[49] D. Rathod and S. Patil, "Security analysis of constrained application protocol (CoAP): IoT protocol," *Int. J. Adv. Stud. Comput. Sci. Eng.*, vol. 6, no. 8, p. 37, Dec. 2017, [Online]. Available: https://www.researchgate.net/profile/Digvijaysinh-Rathod-2/publication/321534413_Security_Analysis_of_Constrained_Application_Protocol_CoAP_IoT_Protocol/links/5a26ca6fa6fdcc8e866e4c34/Security-Analysis-of-Constrained-Application-Protocol-CoAP-IoT-Protocol
[50] M. Kolisnyk, "Vulnerability analysis and method of selection of communication protocols for information transfer in Internet of Things systems," *Radioelectron. Comput. Syst.*, no. 1, pp. 133–149, Feb. 2021, doi: 10.32620/reks.2021.1.12.
[51] A. Cho, T. Kim, C. K. Kim, S. Choi, and S. Lee, "IoT data dissemination scheme for reducing delay in multi-broker environments," *Internet of Things*, vol. 25, p. 101025, Apr. 2024, doi: 10.1016/j.iot.2023.101025.
[52] J. Roldán-Gómez, J. Carrillo-Mondéjar, J. M. Castelo Gómez, and S. Ruiz-Villafranca, "Security Analysis of the MQTT-SN Protocol for the Internet of Things," *Appl. Sci.*, vol. 12, no. 21, p. 10991, Oct. 2022, doi: 10.3390/app122110991.
[53] P. Papageorgas *et al.*, "Wireless Sensor Networking Architecture of Polytropon: An Open Source Scalable Platform for the Smart Grid," *Energy Procedia*, vol. 50, pp. 270–276, Dec. 2014, doi: 10.1016/j.egypro.2014.06.033.
[54] D. Z. Fawwaz, S.-H. Chung, C.-W. Ahn, and W.-S. Kim, "Optimal Distributed MQTT Broker and Services Placement for SDN-Edge Based Smart City Architecture," *Sensors*, vol. 22, no. 9, p. 3431, Apr. 2022, doi: 10.3390/s22093431.
[55] C.-S. Park and H.-M. Nam, "Security Architecture and Protocols for Secure MQTT-SN," *IEEE Access*, vol. 8, pp. 226422–226436, Dec. 2020, doi: 10.1109/ACCESS.2020.3045441.
[56] A. Cimmino *et al.*, "A scalable, secure, and semantically interoperable client for cloud-enabled Demand Response," *Futur. Gener. Comput. Syst.*, vol. 141, pp. 54–66, Apr. 2023, doi: 10.1016/j.future.2022.11.004.
[57] E. Shahri, P. Pedreiras, and L. Almeida, "Extending MQTT with Real-Time Communication Services Based on SDN," *Sensors*, vol. 22, no. 9, p. 3162, Apr. 2022, doi: 10.3390/s22093162.
[58] I. Ungurean and N. C. Gaitan, "A Software Architecture for the Industrial Internet of Things—A Conceptual Model," *Sensors*, vol. 20, no. 19, p. 5603, Sep. 2020, doi: 10.3390/s20195603.
[59] S. Saxena, H. E. Z. Farag, and N. El-Taweel, "A distributed communication framework for smart Grid control applications based on data distribution service," *Electr. Power Syst. Res.*, vol. 201, p. 107547, Dec. 2021, doi: 10.1016/j.epsr.2021.107547.
[60] R. Cruz Huacarpuma, R. De Sousa Junior, M. De Holanda, R. De Oliveira Albuquerque, L. García Villalba, and T.-H. Kim, "Distributed Data Service for Data Management in Internet of Things Middleware," *Sensors*, vol. 17, no. 5, p. 977, Apr. 2017, doi: 10.3390/s17050977.
[61] W. Sim, B. Song, J. Shin, and T. Kim, "Data Distribution Service Converter Based on the Open Platform Communications Unified Architecture Publish–Subscribe Protocol," *Electronics*, vol. 10, no. 20, p. 2524, Oct. 2021, doi: 10.3390/electronics10202524.
[62] A. Alaerjan, "Formalizing the Semantics of DDS QoS Policies for Improved Communications in Distributed Smart Grid Applications," *Electronics*, vol. 12, no. 10, p. 2246, May 2023, doi: 10.3390/electronics12102246.
[63] B. Al-Madani, A. Al-Roubaiey, and Z. A. Baig, "Real-Time QoS-Aware Video Streaming: A Comparative and Experimental Study," *Adv. Multimed.*, vol. 2014, pp. 1–11, 2014, doi: 10.1155/2014/164940.
[64] A. Cilfone, L. Davoli, L. Belli, and G. Ferrari, "Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies," *Futur. Internet*, vol. 11, no. 4, p. 99, Apr. 2019, doi: 10.3390/fi11040099.
[65] K. Liu, "Performance evaluation of zigbee network for embedded electricity meters." Dec. 17, 2009. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:571735
[66] S. Tsakalidis, G. Tsoulos, D. Kontaxis, and G. Athanasiadou, "Design and Implementation of a Versatile OpenHAB IoT Testbed with a Variety of Wireless Interfaces and Sensors," *Telecom*, vol. 4, no. 3, pp. 597–610, Aug. 2023, doi: 10.3390/telecom4030026.
[67] I. Ahonen, "Internet of Things: Wireless Technologies in Home Automation Solutions," 2015. [Online]. Available: https://jyx.jyu.fi/handle/123456789/45101

[68] C. Braghin, M. Lilli, and E. Riccobene, "A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study," *Comput. Secur.*, vol. 127, p. 103037, Apr. 2023, doi: 10.1016/j.cose.2022.103037.
[69] S. Chakraborty, K. Mali, and S. Chatterjee, "Edge Computing Based Conceptual Framework for Smart Health Care Applications Using Z-Wave and Homebased Wireless Sensor Network," in *Mobile Edge Computing*, A. Mukherjee, D. De, S. K. Ghosh, and R. Buyya, Eds. Cham: Springer International Publishing, 2021, pp. 387–414. doi: 10.1007/978-3-030-69893-5_16.
[70] N. M. Obiri and H. Shikunzi, "Long-Range Wide Area Network (LoRa-WAN) Connectivity and Range Evaluation in a Rural Setting," *Int. J. Comput. Appl.*, vol. 185, no. 3, pp. 61–67, Apr. 2023, doi: 10.5120/ijca2023922699.
[71] E. Sisinni, D. F. Carvalho, and P. Ferrari, "Emergency Communication in IoT Scenarios by Means of a Transparent LoRaWAN Enhancement," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10684–10694, Oct. 2020, doi: 10.1109/JIOT.2020.3011262.
[72] C. Delgado, J. M. Sanz, C. Blondia, and J. Famaey, "Batteryless LoRaWAN Communications Using Energy Harvesting: Modeling and Characterization," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2694–2711, Feb. 2021, doi: 10.1109/JIOT.2020.3019140.
[73] M. Jouhari, N. Saeed, M.-S. Alouini, and E. M. Amhoud, "A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 3, pp. 1841–1876, 2023, doi: 10.1109/COMST.2023.3274934.
[74] A. Seferagić, J. Famaey, E. De Poorter, and J. Hoebeke, "Survey on Wireless Technology Trade-Offs for the Industrial Internet of Things," *Sensors*, vol. 20, no. 2, p. 488, Jan. 2020, doi: 10.3390/s20020488.
[75] H. Hanaffi, R. Mohamad, S. I. Suliman, M. Kassim, N. M. Anas, and A. Z. A. Bakar, "Single-Channel LoRaWAN Gateway for Remote Indoor Monitoring System: An Experimental," in *2020 8th International Electrical Engineering Congress (iEECON)*, Mar. 2020, pp. 1–4. doi: 10.1109/iEECON48109.2020.229479.
[76] H. Alqurashi, F. Bouabdallah, and E. Khairullah, "SCAP SigFox: A Scalable Communication Protocol for Low-Power Wide-Area IoT Networks," *Sensors*, vol. 23, no. 7, p. 3732, Apr. 2023, doi: 10.3390/s23073732.
[77] R. Brotzu, P. Aru, M. Fadda, and D. Giusto, "Urban SigFox-based Mobility System," in *2021 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Aug. 2021, pp. 1–4. doi: 10.1109/BMSB53066.2021.9547120.
[78] A. Ortega i Blasi, "Evaluating Thread protocol in the framework of Matter," Universitat Politècnica de Catalunya, 2022. [Online]. Available: https://upcommons.upc.edu/handle/2117/376955
[79] H.-S. Kim, S. Kumar, and D. E. Culler, "Thread/OpenThread: A Compromise in Low-Power Wireless Multihop Network Architecture for the Internet of Things," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 55–61, Jul. 2019, doi: 10.1109/MCOM.2019.1800788.
[80] I. Unwala, Z. Taqvi, and J. Lu, "Thread: An IoT Protocol," in *2018 IEEE Green Technologies Conference (GreenTech)*, Apr. 2018, pp. 161–167. doi: 10.1109/GreenTech.2018.00037.
[81] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N. B. Carvalho, "Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment," *Sensors*, vol. 20, no. 22, p. 6420, Nov. 2020, doi: 10.3390/s20226420.
[82] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020, doi: 10.3390/app10124102.
[83] S. R. Siraparapu and S. Azad, "Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 10, p. 100798, Dec. 2024, doi: 10.1016/j.prime.2024.100798.
[84] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2019, doi: 10.1109/COMST.2018.2867288.
[85] H. Xu, Y. Li, O. Balogun, S. Wu, Y. Wang, and Z. Cai, "Security Risks Concerns of Generative AI in the IoT," *IEEE Internet Things Mag.*, vol. 7, no. 3, pp. 62–67, May 2024, doi: 10.1109/IOTM.001.2400004.
[86] C. Theisen, N. Munaiah, M. Al-Zyoud, J. C. Carver, A. Meneely, and L. Williams, "Attack surface definitions: A systematic literature review," *Inf. Softw. Technol.*, vol. 104, pp. 94–103, Dec. 2018, doi: 10.1016/j.infsof.2018.07.008.
[87] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.
[88] M. Msgna, "Anatomy of attacks on IoT systems: review of attacks, impacts and countermeasures," *J. Surveillance, Secur. Saf.*, vol. 3, no. 4, pp. 150–73, Dec. 2022, doi: 10.20517/jsss.2022.07.
[89] A. Alhusayni, V. Thayananthan, A. Albeshri, and S. Alghamdi, "Decentralized Multi-Layered Architecture to Strengthen the Security in the Internet of Things Environment Using Blockchain Technology," *Electronics*, vol. 12, no. 20, p. 4314, Oct. 2023, doi: 10.3390/electronics12204314.
[90] W. Fei, H. Ohno, and S. Sampalli, "A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions," *ACM Comput. Surv.*, vol. 56, no. 5, pp. 1–40, May 2024, doi: 10.1145/3625094.
[91] Unit 42, "2020 Unit 42 IoT Threat Report," *Unit 42*. Dec. 17, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/
[92] J. Coelho and L. Nogueira, "Enabling Processing Power Scalability with Internet of Things (IoT) Clusters," *Electronics*, vol. 11, no. 1, p. 81, Dec. 2021, doi: 10.3390/electronics11010081.
[93] N. S. Mtetwa, P. Tarwireyi, A. M. Abu-Mahfouz, and M. O. Adigun, "Secure Firmware Updates in the Internet of Things: A survey," in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, Nov. 2019, pp. 1–7. doi: 10.1109/IMITEC45504.2019.9015845.
[94] H. Taherdoost, "Security and internet of things: benefits, challenges, and future perspectives," *Electronics*, vol. 12, no. 8, p. 1901, Dec. 2023, [Online]. Available: https://www.mdpi.com/2079-9292/12/8/1901
[95] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of Smart-Home Security Using the Internet of Things," *Electronics*, vol. 13, no. 16, p. 3343, Aug. 2024, doi: 10.3390/electronics13163343.
[96] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.