Emerging Threats in Internet-of-Things (IoT) Hardware Security

Hashim Elshafie [1], Mosab Hamdan[2], Sayeed Salih[3], Refan Mohamed Almohamedh[3], Ala Eldin Abdallah Awouda[4], Abdelwahed Motwakel[3]

[1]Department of computer Engineering, College of Computer Science, King Khalid University, Main Campus Al farah Abha 61421, Kingdom of Saudi Arabia KSA.
[2]School of Computing, National College of Ireland, Dublin, Ireland
Walton Institute for Information and Communication Systems Science, South East Technological University, Waterford, Ireland.
[3]Department of Management Information Systems, College of Business Administration in Hawtat bani Tamim, Prince Sattam bin Abdulaziz University, Saudi Arabia;
[4]University of Bisha,College of engineering, Department of Mechanical engineering, Bisha, KSA,

Abstract
The Internet of Things (IoT) connects devices into an intelligent, interconnected network, offering convenience and efficiency but also exposing significant vulnerabilities. This discussion highlights IoT hardware weaknesses, emphasizing risks to devices, networks, users, and systems. The most common concern is unauthorized access to sensitive information, but safety risks, such as compromised cars, drones, or medical devices, are even more alarming. IoT's growth has empowered hackers, as seen in a DDoS attack that disrupted internet services across the U.S. East Coast, affecting major platforms like Twitter. Phishing and cyberattacks on IoT-connected devices enable hackers to infiltrate entire networks. As IoT systems increasingly rely on cloud-based intelligence, security gaps and user errors exacerbate risks. This overview explores IoT hardware threats, their implications, and strategies to mitigate system breaches, ensuring safer adoption of IoT technologies.

Keywords:
Internet-of-Things IOT, Hardware Security, IoT network attacks, Application-specific integrated circuit (ASIC) and IOT Ecosystem..

1. Introduction

The Internet-of-Things (IoT) is increasingly becoming an important technology in a variety of sectors, including industries such as agriculture, transport, and healthcare. As its significance continues to grow, IoT technologies and ecosystems are advancing toward a more comprehensive, networked, and connected future. In an interconnected IoT ecosystem, individual devices are linked through a network, which facilitates data sharing, aggregation, and analysis that can enhance the efficiency and functionality of various applications [1][2]. However, this rapid integration of devices also brings forth a myriad of security challenges that must be addressed to protect sensitive data and ensure the integrity of the network. In this work, we will explore the emerging threats in IoT hardware security and discuss potential strategies for mitigating these risks [3]. However, it also poses significant challenges to privacy and other safety-sensitive aspects. Insecure practices that occur during the development and deployment of IoT devices can result in catastrophic consequences for users and systems alike. For instance, from just one vulnerable light bulb, an attacker can effortlessly pivot through all available insecure devices, giving them the means to take over critical systems such as alarm systems or even energy networks, leading to severe repercussions. The interconnected nature of these devices amplifies the potential for widespread disruption [4].

The Internet of Things (IoT) is transforming the world into a smarter, more connected environment where everything becomes rapidly and efficiently accessible. Some examples of IoT applications are illustrated in Figure 1. Industries are increasingly making swift investments in projects driven by the growth and maturity of IoT technologies. Concurrently, IoT is enhancing the quality of our lives and fostering global adoption of these innovations. As user experience (QoE) and application service quality (QoS) requirements continue to rise, researchers are actively developing new strategies to address these demands.

As depicted in Figure 1, IoT applications span a wide range of domains, including real-time multimedia, IoT-enabled healthcare systems, next-generation smart industries, and smart agriculture. Meeting application-specific requirements, alongside addressing security concerns, is a crucial challenge,

Manuscript received April 5, 2025
Manuscript revised April 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.4.3

especially in scenarios such as pandemics that demand rapid data analysis and predictive capabilities. Furthermore, issues related to access technologies, such as spectrum scarcity, pose significant challenges in efficiently allocating resources among a massive number of IoT devices. One promising solution lies in leveraging AI-based technologies to enable dynamic and adaptive systems that optimize resource sharing and address these challenges effectively.

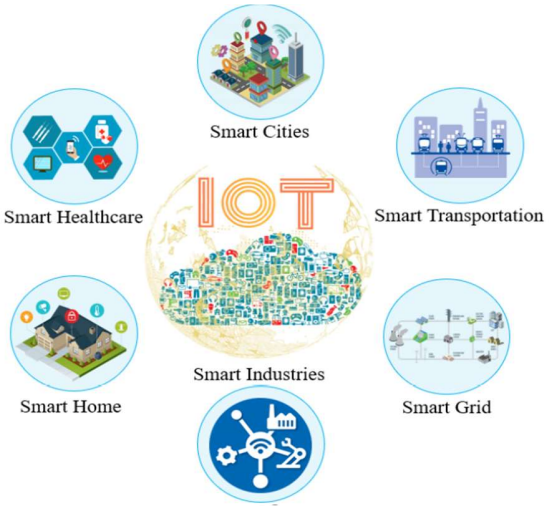

Figure 1. Next-generation Internet of Things (IoT)-based applications [1]

The secure design principles grow in importance, but it is not only up to manufacturers to ensure the security of IoT devices; consumers must also become more aware of the risks and educated about countermeasures. This work aims to highlight the critical vulnerabilities that arise from the rapid proliferation of IoT devices in everyday life. As these devices become more integrated into our daily routines, the potential for exploitation increases, necessitating a more proactive approach to security [5]. This trend underscores the importance of identifying vulnerabilities within the IoT ecosystem, as attackers continuously develop more sophisticated methods to breach security measures. As the number of connected devices continues to grow, the attack surface expands, leading to a heightened risk of breaches that can compromise user privacy and safety Consequently, it becomes imperative to implement robust security protocols and practices to safeguard these devices. provides a comprehensive overview of emerging threats regarding IoT hardware security. Hardware security threats such as clones and counterfeits, overproduction, side-channel attacks, and hardware trojans are investigated and discussed focusing on their effects and countermeasures. The list of countermeasures from manufacturers focuses on proactive security measures during the design and production of devices that increase resilience against emerging hardware attacks; remembered IoT hardware threats and possible countermeasures for consumers [6][7].

2. Overview of IoT Hardware Vulnerabilities

The hardware of Internet-of-Things (IoT) devices are never free of vulnerabilities. One significant reason is that manufacturers releasing new devices often have no failed-safe procedure or old/similar work to follow, which can lead to flawed insecure hardware design. The machines often create them by the tottering workforce or even clueless about secure electronic contrivances [8]. It is often also with the general idea that the components can be exploited instead, which is frequently more comfortable and gives broader options for possible security threats. Another crucial reason is that those sometimes naked, but mostly hidden and able to sense other ways of exploitation vulnerabilities cannot be patched by a software or firmware repair, and neither can be “robustly” fixed during a device usage [9].

We examine the various types of IoT network attacks and analyze their techniques, implications, and potential solutions. IoT attacks can be classified from different perspectives, such as their impact on the core principles of information security (confidentiality, integrity, and availability) or their effect on specific network layers (application, transport, or data link). However, in this paper, we have categorized threats based on the consequences or potential impact of an attack. As shown in Figure 2, these attacks are broadly divided into passive and active attacks. IoT network attacks are diverse, and in this study, we have classified them into 11 types: 2 under passive attacks and 9 under active attacks. Passive attacks are non-intrusive, leaving no network trace, as the attacker primarily eavesdrops on device communication to gather information about the target. Conversely, active attacks involve the attacker actively generating packets, either directly or indirectly, to compromise the target device.

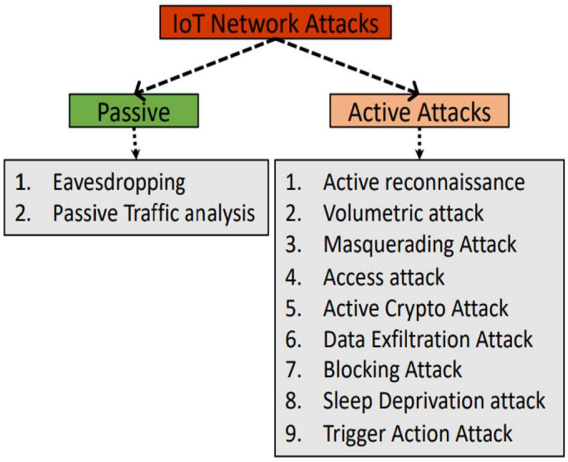

Figure 2. Taxonomy of IoT network attacks [8]

Therefore, IoT hardware vulnerabilities can seriously limit the overall efficiency and security of a system. These vulnerabilities can significantly influence various aspects of the designed system, which include critical elements like battery life, security protocols, user privacy, and the overall total cost of the product. As we delve deeper into the subsequent text, a comprehensive outline, along with a clear view of the examined topics, will be provided. We will explore how these vulnerabilities can be exploited by malicious actors, thereby posing risks that need to be effectively managed to ensure robust protection against potential threats In particular, we will highlight the critical areas where IoT devices are susceptible, such as inadequate authentication mechanisms, insecure firmware updates, and vulnerabilities in communication protocols. By understanding these weaknesses, we can better prepare for the challenges that arise in securing IoT hardware [10][11].

The text is meticulously organized into several key sections that cover distinct yet interconnected topics about cybersecurity and hardware safety. First, it delves into (1) Insecure Hardware Design, which encompasses critical discussions about the inherent flaws present in hardware design as well as various instances of flaws resulting from hardware failures; this section aims to highlight potential vulnerabilities that could be exploited. Next, it advances to (2) Side-Channel Attacks, where readers are provided with a comprehensive overview, along with a detailed explanation of the underlying concept, and illustrative worked example attacks that elucidate the nature and impact of these attacks on systems [82]. Following this, (3) Hardware Trojans are explored, giving an overview along with descriptions of different types and working examples of malicious design that are often hidden within legitimate hardware—these Trojans represent serious threats. Moving on, (4) Counterfeit and Cloned Devices are examined, which includes an insightful overview detailing how these compromised items not only pose risks to users but also discuss the strategies that malicious actors employ to profit from selling such devices. Finally, the document wraps up with five conclusions, summarizing the critical points covered while reflecting on the larger implications of the findings. Surveys of existing literature are integrated throughout, primarily centering on the availability of academic resources for further reading, as well as addressing the practical limitations that researchers face within this field. Special attention is given to the difficulties associated with having vectorized text to successfully train an initial implementation of threat detection systems in the ever-evolving landscape of hardware security [83].

2.1. Insecure Hardware Design

Application-specific integrated circuit (ASIC)-based devices demonstrate a remarkable level of susceptibility to a range of significant hardware vulnerabilities. This vulnerability is primarily a consequence of poor implementation either of the original design itself or of the underlying protocol stack upon which they rely. In fact, it is noteworthy that a large majority of Internet of Things (IoT) devices are deliberately constructed with the intention of being low-cost solutions, which ultimately leads to the incorporation of minimal to no additional security features beyond those default settings established at the factory [12]. This particular design philosophy frequently tends to overlook many critical aspects of security, ultimately resulting in hardware that becomes highly susceptible to various forms of exploitation and malicious activities. As a direct consequence, attackers can effectively leverage these vulnerabilities to gain unauthorized access to sensitive data, manipulate device functionality, or even launch far larger and more complicated attacks on interconnected networks. This ongoing design philosophy often prioritizes cost reduction over robust security measures, therefore leaving numerous

devices significantly vulnerable to a wide array of attacks. As a result, attackers are able to exploit these inherent weaknesses. This enables them to gain unauthorized access, disrupt essential services, or compromise user data, threatening overall system integrity and user trust [13].

Moreover, the distinct lack of secure update mechanisms significantly exacerbates the current situation, making it increasingly difficult to promptly patch known vulnerabilities after deployment. This prevalent situation highlights the urgent need for manufacturers to prioritize and emphasize security right from the design phase, incorporating essential features such as robust hardware-based encryption and reliable secure boot mechanisms. By proactively addressing these vulnerabilities early in the comprehensive development process, the entire IoT ecosystem can become far more resilient against a wide array of potential attacks and threats, ensuring greater safety and integrity for all connected devices that compromise the integrity of the entire network. Consequently, manufacturers must prioritize robust hardware security measures during the design phase, ensuring that devices are resistant to various forms of attack, including physical tampering and unauthorized firmware modifications. This proactive approach is essential to safeguard not only individual devices but also the broader ecosystem of interconnected IoT products [14]. This trend not only compromises the integrity of the devices but also poses significant risks to the entire network they are part of. As a result, attackers can exploit these weaknesses to gain unauthorized access, leading to data breaches and other malicious activities Moreover, the reliance on cost-cutting measures often results in outdated or vulnerable components being utilized, leaving devices susceptible to attacks that could have been easily mitigated with proper design considerations. This lack of foresight not only affects individual devices but can also create cascading vulnerabilities within interconnected systems [15].

This deliberate cost-cutting approach can result in serious security risks, emphasizing the need for enhanced attention to secure design processes and highlighting the importance of establishing a framework that prioritizes security from the initial design phase. This necessitates a shift in the mindset of manufacturers, who often prioritize cost over security, to recognize that investing in robust security measures can ultimately safeguard their products and users. Such a transformation is crucial in order to mitigate the vulnerabilities inherent in IoT devices, which can be exploited by malicious actors to gain unauthorized access and control over connected systems. By adopting a security-first approach, manufacturers can not only protect their intellectual property but also enhance consumer trust and compliance with regulatory standards that will ultimately lead to a more resilient IoT ecosystem [11].

This approach should encompass not only the critical design phase but also the comprehensive lifecycle of the device, ensuring that robust security measures are seamlessly integrated from the ground up. Moreover, collaboration between manufacturers, security experts, and regulatory bodies can effectively foster an environment where best practices are continuously shared and universally implemented. This proactive approach not only mitigates the risk of vulnerabilities being inadvertently introduced during the design stage but also addresses a multitude of potential threats that may arise during the manufacturing processes, deployment stages, and eventual decommissioning of the devices. By prioritizing security at every phase of development and operation, we can significantly reduce the attack surface, enhance the overall resilience of IoT devices against emerging threats, and ensure a safer technological landscape for all users [16]

This often involves the use of globally shared keys, or, alarmingly, it can also include the practice of leaving these critical keys wholly unsecured altogether. Moreover, the prolonged manufacturing time associated with ASIC devices creates a complex scenario where any necessary changes to address potential vulnerabilities cannot be made at all once the manufacturing process has concluded, further exacerbating the already pressing security issues. When these vulnerabilities are exploited, it can lead to extremely dire situations in which unauthorized entities are enabled to read, modify, or even inject harmful and malicious data into the external interfaces of the devices. This not only compromises the overall integrity of the device but can also significantly affect its proper operation and raise serious concerns regarding the safety of users and the protection of data security. Consequently, developers and manufacturers must remain vigilant in addressing these risks

proactively to ensure a secure and trustworthy manufacturing process [17].

Security features usually added to firmware are often poor and do not make the hardware implementation any safer [18]. Attacks can be launched at all stages of an IoT device lifecycle from the deployment stage, to the update process and data management. Examples of such hardware attacks, affecting the power of the targeted device include current consumption increase attacks, power supply manipulation, or corruption of power control circuits. Unprotected or poorly protected debug interfaces can easily lead to hacking the device. Furthermore, in distributed IoT systems that contain more than one device, physical access to even a single one can cause a domino effect that would lead to a chain reaction bringing down the remainder, complicating the system reboot and possibly causing operation loss until they are replaced or fixed [19].

This suggests that even the most well-protected devices can potentially become vulnerable points in a network if they are connected to other devices that are unprotected or inadequately protected. Device fail-over mechanisms can offer a solution to this issue, but they are frequently non-implementable due to various factors inherent in the devices themselves. While the examples provided above are not exhaustive and serve mainly as illustrative cases, they effectively demonstrate how even a seemingly simple attack can bring down a commercial device with ease. The nature of these attacks, being performed on fixed structures, emphasizes the critical importance of designing hardware from the ground up in collaboration with security experts and professionals in the field [20]. It is absolutely essential to exercise special care and consideration when defining the external interfaces of any device, as these particular interfaces often reveal critical hardware vulnerabilities and consequently serve as the first potential targets for an attacker who is seeking to exploit any weakness. By integrating comprehensive security considerations from the very earliest stages of hardware design, manufacturers can significantly enhance the protection of devices against not only known threats but also against emerging, novel attacks that exploit newly discovered vulnerabilities in the system. Recognizing and effectively addressing these significant issues is vital in safeguarding not just individual devices, but also the overall integrity and security of entire systems. This attentiveness to security at the foundational level can lead to a more resilient and trustworthy technological environment for users and organizations alike [21].

Security Policies:

A cybersecurity policy is a framework of standardized procedures and processes designed to safeguard an organization's network. The management of these policies involves identifying, implementing, and overseeing their rules, methods, and guidelines. Regularly updating these policies by assessing new IT assets and resources ensures protection against emerging threats. Organizations should implement various policies to maintain effective cybersecurity controls, such as an Acceptable Use Policy, a Data Breach Response Policy, a Disaster Recovery Plan, a Business Continuity Plan, a Remote Access Policy, and an Access Control Policy. Figure 3 illustrates the enforcement of a security policy within an enterprise, demonstrating how it serves as a barrier between access management modules and system resources.

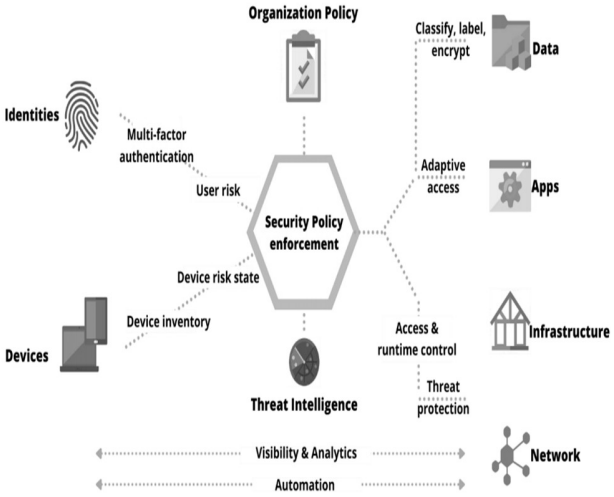

Figure 3 . Security policy enforcement in an enterprise.

2.2. Side-Channel Attacks

Side-channel attacks take advantage of vulnerabilities found in the hardware components of Internet of Things (IoT) devices. These attacks achieve this by analyzing indirect leakages of information, such as variations in power consumption, electromagnetic emissions, or timing discrepancies that can expose critical information regarding the

underlying security mechanisms of a device or its confidential data. In contrast to traditional attacks, side-channel attacks possess a statistical nature, wherein they focus on observing and analyzing a large number of executions to gather relevant data. They are predicated on the leakage model hypothesis, which posits that secret-dependent intermediate values can inadvertently disclose extra information during the cryptographic operations executed by a physical device [22].

To effectively counteract these various types of attacks, a multitude of innovative masking techniques have been proposed that specifically aim to obscure and protect the internal states within the device. However, the foundational premise underlying side-channel attacks—that a physical attack must occur for the analysis to be genuinely effective—may not hold true within the specific context of the Internet of Things (IoT) due to the unique characteristics of IoT devices. Unlike traditional systems, IoT devices often operate in resource-constrained environments, which can limit the effectiveness of conventional countermeasures. Furthermore, the interconnected nature of IoT ecosystems presents additional challenges, as attackers can exploit vulnerabilities across multiple devices to obtain sensitive information without direct physical access. This is primarily due to the inherent characteristics of these devices, which often operate in an unprotected and vulnerable real-world environment. Despite the implementation of such defenses, advanced side-channel attacks can still be executed successfully, as there exist various forms of additional leakages that occur outside the immediate physical confines of the device itself such as electromagnetic emissions, power consumption fluctuations, or even timing variations [23].

These leakages can provide an adversary with critical information that may be leveraged to compromise the device's integrity, confidentiality, or availability. Consequently, researchers and practitioners are continuously working to develop more robust countermeasures to mitigate the risks posed by these sophisticated attacks.. A prime example of this phenomenon is the electromagnetic signals that are emitted during their operational processes, which remain impossible to effectively guard against using purely software-based countermeasures alone. The challenge becomes even more pronounced when considering the diverse range of attack vectors that adversaries may exploit, thereby highlighting the urgent need for robust and multidimensional security measures that extend beyond traditional methodologies to safeguard against these vulnerabilities. For instance, physical shielding techniques can help mitigate the risk of side-channel attacks by obstructing the leakage of electromagnetic signals. Additionally, implementing hardware-level encryption can provide an extra layer of protection, making it significantly more challenging for attackers to extract sensitive information through these channels [24][25].

As the Internet-of-Things (IoT) continues to evolve, a range of emerging threats to hardware security has become increasingly prominent, posing significant challenges for manufacturers and users alike.In fact, successful practical attacks have been demonstrated that exploit these electromagnetic leakages. These attacks, categorized as non-invasive side-channel attacks, are capable of retrieving complete AES-128 secret keys, doing so with only 200 measurements. What makes these attacks particularly alarming is that the same methodology can be employed to extract an encryption key within a remarkably short timespan of a minute while achieving a success rate that approaches 100%. This capability underscores the sophistication and effectiveness of side-channel attacks in the realm of IoT security [26] .This is particularly concerning for IoT devices, which often lack adequate defenses against such vulnerabilities. The reliance on minimal hardware resources and the prevalence of low-cost components make these devices attractive targets for attackers. Moreover, as IoT devices become increasingly integrated into critical infrastructure, the potential impact of successful side-channel attacks escalates dramatically [27]

The most efficient techniques in this field require processing only 16 traces to produce meaningful results. This highlights the capabilities of electromagnetic non-invasive side-channel attacks and emphasizes their significance as potential threats within the rapidly evolving context of the Internet of Things (IoT). These techniques showcase vulnerabilities that necessitate due consideration. To the best of our knowledge, utilizing electromagnetic emissions, we find that only the smallest number of traces, which is 200, was necessary to successfully disclose sensitive 128-bit key information for implementations that have been commercially

mainstreamed [28]. Furthermore, this document includes brief introductory descriptions regarding electromagnetic emissions, specifically addressing the types of measurement equipment utilized in such analyses. It is crucial that this issue garners the attention of a wide range of stakeholders, including designers and implementers of IoT devices, as well as users and policy-makers who are engaged with the formulation of regulations that significantly impact aspects of privacy, security, and safety. While no foolproof solutions can provide an absolute, universal guarantee of security, certain countermeasures may be implemented to either inflate the costs associated with attacks or diminish their probability of achieving success Moreover, it is essential to foster collaboration among these groups to share insights and develop effective strategies against side-channel attacks, which exploit unintended information leakage during the operation of IoT devices. Initiatives such as workshops and forums can facilitate knowledge transfer, enabling stakeholders to better understand the vulnerabilities present in their systems [29]

Existing literature has proposed various hardware techniques aimed at concealing sensitive information from potential electromagnetic eavesdroppers. These include the use of specialized chips designed for intentional high-speed operations, the integration of Faraday cages, and the incorporation of ferromagnetic materials to enhance security. Beyond traditional methods, more innovative and speculative approaches involve the utilization of certain metamaterials, or the development of devices based on silicon-on-nothing technology, which effectively isolates active regions within specific silicon dies. As a result, when numerous measurements are required, the process can become not only impractical but also extremely costly, which discourages the perpetration of such attacks. It may be reasonably anticipated that the continually increasing number of applications and services associated with IoT devices will drive further research and investment into protective measures against side-channel threats Furthermore, as IoT technology evolves, the sophistication of these attacks is likely to increase, necessitating frequent updates to security protocols and methodologies [30].

Researchers and developers must adopt a proactive approach in order to mitigate risks associated with side-channel vulnerabilities to effectively counteract these threats. This includes not only the implementation of advanced encryption techniques but also the development of hardware-based defenses that can detect and respond to side-channel attacks in real time. Moreover, collaboration between industry stakeholders and academic researchers will be crucial in establishing best practices and standards that can be adopted across various IoT implementations. This quest would not be limited to securing individual components but would extend to ensuring the integrity of the entire system's architecture, including enclosures that effectively mask or block the potentially harmful electromagnetic leakages [31]. In addition, there is a pressing need for the development of supplementary solutions that can enhance the privacy of users' activities, thus protecting them from the dangers of remote interception. There exists considerable space for future research endeavors that concentrate on gathering extensive volumes of electromagnetic data in real-world conditions, exploring the feasibility of employing alternative unconventional methods to exploit such information, or examining the broader context of deriving unique characteristics of devices from numerous small electromagnetic leakages [32].

Real-time monitoring of data generated by smart devices and their transmission within an interconnected system is crucial for intelligent decision-making. These advanced systems operate autonomously, without human intervention, making decisions in real-time to address specific threats by adapting to changing environmental conditions. Figure 4 illustrates a secure smart healthcare management system leveraging technologies such as artificial intelligence, blockchain, machine learning, and deep learning to enable autonomous operations and decision-making. Sensors collect patient data and transmit it to microprocessors, which are linked to wireless communication technologies for routing and forwarding the data through gateways. This data is then stored in virtual machines, commonly referred to as clouds, for preprocessing and analysis. The processed information is accessible to doctors, experts, and patients. Nevertheless, robust security mechanisms are essential to safeguard the system against potential threats from adversaries.

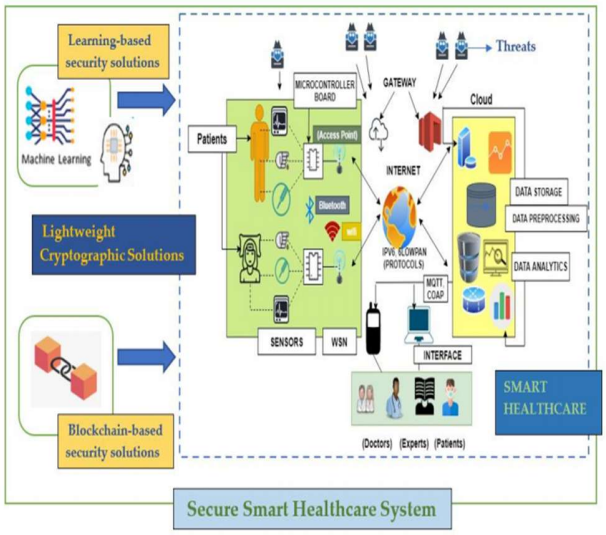

Figure 4. Secure Smart Healthcare System.

2.3. Hardware Trojans

Cyber-Physical Systems (CPSs) are networks of closely interconnected computing and physical components that are used in a growing number of critical applications. These systems have the capacity to monitor and automatically respond to physical events in industrial machines and critical infrastructure. With the advent of programmable application-specific integrated circuit (ASIC) variants like field-programmable gate arrays (FPGAs) and the continuous advancements in the arena of integrated circuits manufacturing, it is now possible to embed such systems in hardware. From an adversary, tampered hardware and/or malicious circuit operation may lead to complete failure in functionality, safety, or security [33]. Employing hardware security methods therefore becomes of high importance to secure such systems. In this way, an adversary tamper or exploit pre-parametric and post fabrication mechanisms present in the supply chain. This manipulation can lead to significant vulnerabilities, allowing the attacker to gain unauthorized access to sensitive data or disrupt the normal operation of IoT devices. As such, understanding the mechanisms behind Hardware Trojans is vital for developing effective security measures in IoT hardware [34].

An Integrated Circuit (IC) typically consists of numerous Intellectual Property (IP) cores, including CPUs, memory units, network-on-chip components, controllers, converters, input/output devices, and more. As ICs become smaller in size, their cost and complexity increase, prompting manufacturers to outsource production overseas to mitigate expenses and streamline processes. This reliance on a global IC production supply chain, however, heightens vulnerability to hardware attacks. The diversity within the supply chain allows adversaries to embed malicious circuitry or code into designs. Figure 5 illustrates a standard IC supply chain, highlighting third-party vendor involvement, lifecycle stages, and market components in blue to represent external entities, while in-house production processes are shown in brown.

Additionally, critical control and communication systems often assume that the underlying hardware is secure a premise that is not always valid. For instance, backdoors can be exploited to manipulate weapon control systems, transportation networks, and nuclear power infrastructure, as noted in. Practical examples of hardware attacks include counterfeit electronics, vulnerabilities in hotel keycards, and flaws in parking payment systems.

The increasing adoption of open-source and commercial tools for modern computing systems, such as FPGA CAD tools, has introduced opportunities for remote attacks, even without physical access to the target. Consequently, computing hardware is becoming increasingly susceptible to emerging security threats. These vulnerabilities can stem from unintentional design flaws, systemic side effects , or deliberate design alterations. The primary objectives of such attacks often include compromising intellectual property, secure systems, machine learning models, and cryptographic operations.

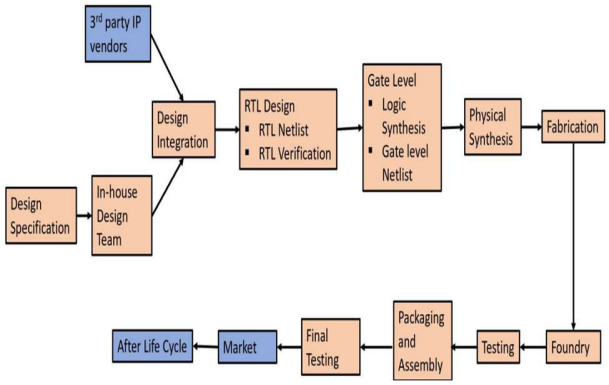

Figure 5. Integrated circuit (IC) design supply chain.

Hardware Trojans also known as malicious modifications, backdoors, or kill switches - are clandestine design alterations in an integrated circuit (IC) resulting in the unintentional, hidden, and 'unexpected' behavior of the impacted IC component. Hardware Trojans are sneaky and pre-planned circuit modifications embedded into the chip design to compromise security or functionality. Since they are illustrated, verified, and tested in hardware, their discovery is challenging. There are various ways in which they can be added to the design, including altering the original layout, a positioning superfluous layers, or exploiting arrangements of the existing components of the device. Apart from that, diverse implementation methods can be used; from static and dynamic comparators encompassing, and under particular circumstances trigger activation, to modifications at transistor-level rendering the chip arbitrarily unfunctional. Such modifications are highly integrated into the design obfuscated by design tools or even placed beneath other circuitry. These modifications are usually triggered by a predefined set of conditions resulting from the measurements of the impacted device. Visually indispensable effects, akin to changing the state of the affected chip, may not take effect, further fortifying the emotive nature of the modification [35].

Supposedly insignificant alterations can result in considerable, device behavior changes. Ultimately, Security threats to the Internet of Things (IoT) devices infiltrated with hardware Trojans present data breach risk in edge IoT ecosystems or can make functional devices go dysfunctional. Time and again, hardware Trojans would not take effect until months later, circumventing the predevaluation steps of the supply chain. However, given the comprehensive control they introduce, the ramifications can be dire. A prosperous business would soon become defunct if the secrets behind the individual competitive advantage became instantly available to the competition. Moreover, the chances of innovation and growth in the ISP market would be stunted indefinitely. Because of the global endeavor to curb this emerging threat, numerous had been reported high-profile incidents involving IC devices, illustrating the extensive nature of these situations. Efforts to mitigate or tackle hardware Trojans assume greater importance. Enhanced design verification and material testing algorithms improve Trojan detection. The transparency and homogeneity between independent links within the industry supply chain are underlined as obligatory to obviate this incongruity. Ultimately, industry expertise should be enlightened about hardware Trojan scourges for the design and use of Safer devices [36].

Figure 6. describe the classic hardware attacks encompass a range of threats targeting integrated circuits (ICs), including hardware Trojans, IP piracy, IC overbuilding, reverse engineering, side-channel attacks, and counterfeiting. Hardware Trojans involve malicious modifications to IC designs, while IP piracy and IC overbuilding exploit unauthorized replication or excess production of ICs. Reverse engineering focuses on extracting a circuit's design or functionality, side-channel attacks leverage physical properties such as power or electromagnetic emissions to compromise sensitive data, and counterfeiting involves the production or distribution of fake or recycled ICs. To combat these threats, countermeasures such as design obfuscation, IC metering, and split manufacturing provide robust protection across multiple attack types by hiding critical design elements, tracking production, and isolating manufacturing steps. Additionally, techniques like physically unlovable functions (PUF), noise injection, IP watermarking, IC camouflaging, and aging sensors address specific vulnerabilities by enhancing security, ensuring authenticity, and reducing information leakage. These multi-layered defenses are essential in safeguarding modern IC supply chains and critical systems against diverse hardware security threats.

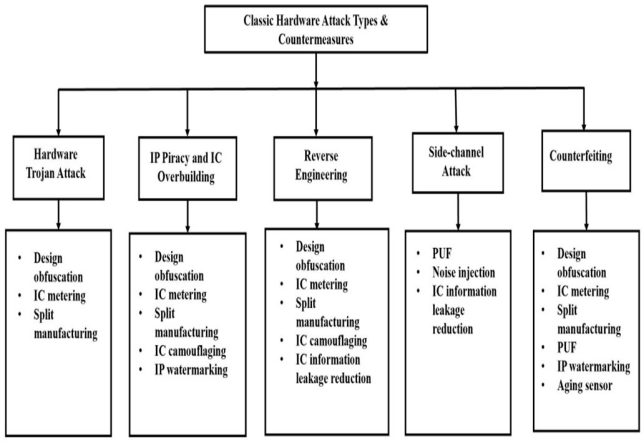

Figure 6. Classic hardware attacks and countermeasures

2.4. Counterfeit and Cloned Devices

A cloned device is a type of device that pre-maturely extracts, alters, or even emulates device-specific information from an authentic device, thereby behaving like an authenticated device within a network environment. Such cloned devices within a network can be conceptualized as an 'attack of entry' since they may gain unauthorized access to the authentication and control schemes that the network owner is implementing. In contrast to counterfeit devices, which are typically classified as unauthorized, copied, or otherwise manipulated products, cloned devices specifically originate from pre-mature extraction, alteration, or emulation of defected products. The economic and operational impacts associated with counterfeit devices are often the focus of attention; however, it is crucial to highlight that cloned devices are considered dead-on-arrival. Consequently, the operational ramifications of cloned devices are often overlooked, which raises significant risks for both consumers and manufacturers alike. The broad proliferation of cloned devices poses a risk of undermining trust in Internet of Things (IoT) systems, instigating vulnerabilities that can be easily exploited by malicious actors in the ecosystem. Furthermore, the increasing prevalence of cloned devices complicates the process of distinguishing between legitimate devices and their cloned counterparts. This growing complexity also presents challenges for regulatory efforts and enforcement measures, as it becomes increasingly difficult to ensure compliance and maintain the integrity of the networked systems involved, as security measures struggle to keep pace with the rapid evolution of IoT technologies. Consequently, the potential for exploitation by malicious actors increases, leading to heightened risks for both consumers and businesses. Organizations must therefore prioritize the development of robust authentication protocols and invest in advanced detection methods to mitigate the threats posed by these counterfeit devices [37][38]

Studies show that new devices can be counterfeited or cloned devices even when they are in packaging. When counterfeit or cloned devices are incorporated into a network without expertise and proper inspection, the network may be silently controlled by the attacker for an unauthorized i.e., attack of entry. Such an unnoticeable network of cloned devices gives the attacker access to all data flow, shared keys, and operational procedures concerning legitimate network devices making him undetectable and unremovable, which can lead to severe security breaches and data loss. To combat this issue, organizations must implement robust authentication mechanisms and continuous monitoring systems that can identify and mitigate the risks associated with these devices [8]. If the ownership of a cloned device network becomes public, the network of cloned devices will be abandoned since the attacker now has no utility. Additionally, it is shown that under real-world circumstances there are extensive legal gaps concerning counterfeit devices. In light of the legal gap, the consumer CERT model is proposed to instigate the responsible actor to act against counterfeit products. This model aims to enhance consumer awareness and encourages the reporting of suspicious products, thereby mitigating the risks associated with counterfeit and cloned devices [39].

Possible attack paradigms of counterfeit and cloned devices are modeled in detail, and key parameters are clearly defined to facilitate a deeper understanding of the potential vulnerabilities. Furthermore, a comprehensive analysis of countermeasures is carried out to illustrate the various strategies that can be employed to mitigate these threats effectively. It is shown that proper inspection and continuous monitoring of the incoming devices play a crucial role in preventing the incorporation of an extensive network of counterfeit devices into legitimate systems. Nonetheless, as this issue gains traction under widespread adoption, the ongoing concern revolves primarily around the authenticity of the device itself; hence, a consumer awareness model is also proposed [40]. This model emphasizes the importance of understanding the main benchmarks deployed and verifying the authenticity of devices to ensure that consumers are well-informed. Black and gray markets have emerged as the most preferred venues for the sale of counterfeit IT hardware, which undoubtedly includes a significant proportion of IoT devices, thereby complicating the challenges faced by manufacturers and legitimate vendors. Due to the inherent nature of these markets, there are very few successful applications to effectively prevent this concerning trend, highlighting the urgency for better regulations and consumer education [30].

3. Emerging Threats in IoT Hardware Security

The evolution of technology has brought an unprecedented increase in the number of devices connected to the Internet. By 2021 over 25 billion devices will be connected wirelessly to the Internet, forming the Internet of Things (IoT). This rapid expansion presents significant challenges, particularly in the realm of hardware security. As more devices connect, the potential for vulnerabilities increases, making IoT hardware an attractive target for cybercriminals. These vulnerabilities can stem from a variety of factors, including inadequate security measures during the design phase, lack of regular updates, and the inherent complexity of device interconnectivity. The variety of devices spans from wearables, health and fitness devices, and cameras, through smart home appliances like thermostats, to industrial solutions such as smart buildings or smart grid infrastructure [8]. Even though the drive behind the IoT revolution was information access and acquisition, an unexpected byproduct was the ecosystem for the creation of more attack vectors. Since the creation and subsequent exploitation of the first worm, the Internet security myth has proven resilient to absolute protection. The same is inevitable for the IoT. Being a sum of all Internet-connected devices, those in the IoT network are threatened by the same attackers targeting servers, phones, or PCs. Thus, automating the identification, assessment and mitigation of these threats is becoming a necessity [41].

Nonetheless, the future of the field is, for the moment, unfortunately obscured by a wide variety of threats that are unidentical to those we encounter in today's ever-evolving world. Such threats will inevitably shape the future of IoT security, but they must first undergo rigorous research in order to be adequately mitigated. By thoroughly following advances in the current state and complementary fields, it is possible to pinpoint a series of emerging threats to the security of the hardware compartment of the IoT that require well-considered and advanced countermeasures. These countermeasures will play a crucial role in ensuring that the integrity of the IoT ecosystem is maintained, safeguarding devices and their networks from potential vulnerabilities that could be exploited in unforeseen ways and adapting to new methodologies in hardware design and communication protocols. Some of the most pressing threats include physical tampering, where malicious actors gain unauthorized access to devices, and the exploitation of weak authentication mechanisms that can lead to unauthorized control over critical infrastructure. Additionally, as IoT devices become more complex, vulnerabilities arising from software dependencies and firmware updates are increasingly being targeted, necessitating a comprehensive approach to security that encompasses not just hardware but also the entire device lifecycle [42].

In the figure 7. Illustrate the Application Layer serves as the interface for end-users, providing services in various domains such as smart homes, smart meters, smart cities, and smart grids. However, this layer is particularly vulnerable to numerous security threats. One such threat is information theft, where attackers target private data stored in IoT applications, which can be mitigated through encryption, authentication, and privacy management protocols. Access control attacks pose a significant risk, as compromised access control systems allow attackers to gain control over entire IoT applications. Service interruption attacks disrupt user access by overwhelming IoT applications, denying legitimate users their services. False code sending attacks, often executed through Cross-Site Scripting (XSS), enable adversaries to manipulate IoT accounts or systems by sending falsified data. Similarly, sniffing attacks exploit insecure network traffic, allowing attackers to extract sensitive user information. Lastly, reprogram attacks target unsecured programming processes, enabling adversaries to rewrite codes, potentially causing the IoT system to malfunction. Implementing robust encryption, authentication, traffic monitoring, and secure programming practices is essential to address these vulnerabilities and ensure the security of IoT applications.

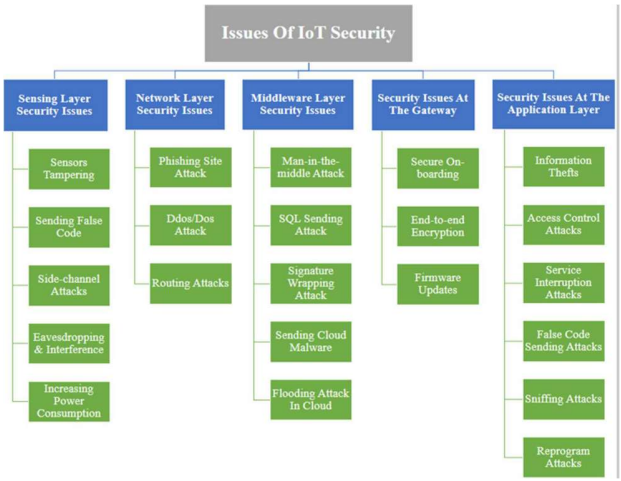

Figure 7. Issues of IoT securities

3.1. Edge Device Exploitation

With the dawn of the fourth Industrial Revolution (Industry 4.0), the exciting prospect of smart interconnected devices known as the Internet-of-Things (IoT) has become an astonishing reality that is revolutionizing many aspects of modern life. Networked "smart" devices now pervade a wide variety of environments in our everyday surroundings: from advanced surveillance cameras and innovative smart refrigerators to sophisticated industrial automation systems, environmental sensors, and health-focused wearables—the list goes on and continues to grow. It is estimated that by the year 2025, there will be over 21 billion smart devices seamlessly integrated into various sectors, ranging from residential housing to complex industrial applications, enhancing connectivity and efficiency across the board [8] . Lately, many IoT devices have been running on edge computing infrastructure, in which the system processes data at the network edge as opposed to a centralized server. This architecture enhances efficiency and responsiveness but also introduces new vulnerabilities. Attackers can exploit weaknesses in the edge devices, gaining unauthorized access to sensitive data and compromising the overall security of the IoT ecosystem [43].

While edge devices have recently brought significant advancement to a variety of applications, they pose an additional layer of vulnerability in current IoT hardware security. Being distributed, edge devices process data close to the data source, effectively reducing the amount of data transferred cross network, and improving response time. However, zero trust device grouping opportunities raised by recent edge computing are indeed non-negligible, in terms of security. Many edge devices used in the implementation of the IoT system concentrate on reading sensor values directly through the Physical Web, thus bypassing the gateway and cloud security mechanisms. Edge devices are more easily accessible by potential attackers and, because of performance trade-offs, they often possess less security measures than in non-edge implementations. Such lack of security could consist of simple oversights like the lack of encrypted connections being made available, limited protection of data-at-rest, and inadequate patch management. Such inadequate security hygiene, when abused, potentially allows attackers to gain unauthorized access to known edge devices in the network, which could later be used to gain access to other devices in the supposed trusted cluster. Such a series of events could leak sensitive data locally stored on the cluster that might have been useful for diagnosis reasons, blind the cluster's sensors data, or selectively inhibit access to specific actuators. Conceptually, this would prevent a node from entering/existing a given configuration, which may disrupt service delivery or impose safety risks [44].

Numerous IoT incidents have taken place in the past that follow edge device exploitation reasoning and similar wide-spread attack scenarios on vulnerable edge devices were verified. Since the IoT system is often a collaborative effort among entities, many edge devices could represent lightweight commodities with performance trade-offs, aiming to reduce costs. It can also be expected that many edge devices often run proprietary software and, as a consequence, do not receive well timely patches that address critical vulnerabilities. This lack of timely updates renders them susceptible to various forms of cyberattacks, including unauthorized access and data breaches. Furthermore, the integration of insecure edge devices into larger IoT ecosystems can amplify the potential impact of these vulnerabilities, leading to widespread disruptions [45]. Given that and previous observations, for that reason, security considerations for the IoT should be revisited, as it is necessary to design security practices suitable for developments in edge computing infrastructure, rather than attempting to only safeguard devices considered to operate on it. Collaborative efforts between IoT and IT security researchers lead to the development of IoT hardware

security frameworks that improve the security posture of the devices, the network infrastructure, and the communication layer. These frameworks could then be adopted by the relevant stakeholders to selectively improve their security domain in the hopes of deterring attackers or raising their cost of launching a successful attack on critical infrastructures. In this light, it is essential to consider models describing attacks, but also providing actionable advice to mitigate such threats. Summarizing, with the rapid uptake of edge computing in industrial and residential applications, a pressing need arises to address the security issues dealing with it and guarantee resilient IoT infrastructures [46].

Edge Computing and Internet of Things (EC-IoT) systems are vulnerable to various attack types, as illustrated in Figure 8. Although recent advancements in artificial intelligence (AI) have greatly enhanced cybersecurity measures, these technologies are particularly adept at addressing specific categories of threats. This paper centers on evaluating AI-driven solutions to counteract these particular attack types. The goal is to showcase the practical applications and advantages of AI in strengthening edge network security by concentrating on a targeted list of specific threats.

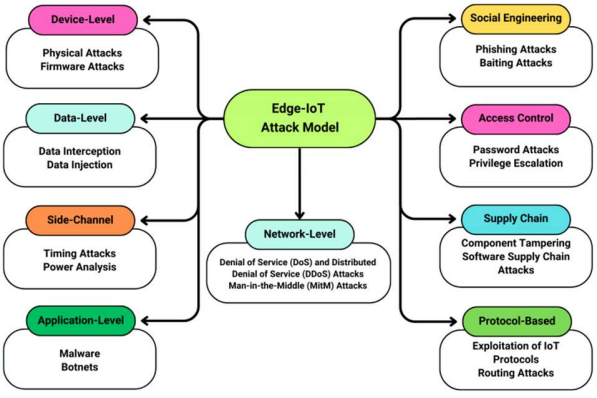

Figure 8. Edge-based IoT attack model with examples of each sub-model

Network-Level Attacks: EC-IoT environments face significant network threats, such as Distributed Denial of Service (DDoS) and Man-in-the-Middle (MitM) attacks. DDoS attacks flood networks with traffic, rendering them inaccessible and disrupting IoT services due to the decentralized edge architecture. MitM attacks, on the other hand, intercept and potentially alter communications between devices, exploiting the wireless nature of EC-IoT connections to gain unauthorized access to sensitive data.

Application-Level Attacks: Malware and botnets pose severe threats at the application layer. Malware infects IoT devices to disrupt functionality, steal data, or enable unauthorized control, while botnets leverage compromised devices to execute large-scale attacks like DDoS, data theft, and malware dissemination, amplifying their impact through the collective power of multiple devices.

Data-Level Attacks: These attacks involve data interception, where attackers eavesdrop on transmissions to steal sensitive information, and data injection, where false data is introduced into communication flows, leading to incorrect decisions or system manipulation, compromising the reliability of IoT systems.

Access Control Attacks: Weak or default passwords and privilege escalation represent critical threats. Password attacks (e.g., brute force or dictionary attacks) aim to gain unauthorized access, while privilege escalation exploits system vulnerabilities to elevate access levels, enabling attackers to control critical functions or data.

Protocol-Based Attacks: Vulnerabilities in communication protocols, such as CoAP, SSDP, and MQTT, can be exploited to disrupt IoT services. Attackers may manipulate routing, neighbor discovery, or transmission protocols to intercept or redirect data, causing congestion, unauthorized access, or data breaches.

Side-Channel Attacks: These exploit physical information leakage, such as power consumption or electromagnetic emissions, to infer sensitive data like encryption keys. Such attacks bypass traditional defenses by analyzing unintended side-channel signals, posing significant security risks.

Supply Chain Attacks: These target vulnerabilities during the manufacturing, distribution, or deployment stages. Attackers may introduce counterfeit components, tamper with hardware or software, or implant malware, compromising the security, availability, and authenticity of IoT devices.
Social Engineering Attacks: By exploiting human vulnerabilities, attackers manipulate individuals into revealing sensitive information, such as login credentials, or performing actions that compromise security. Tactics include phishing, impersonation, and

pretexting, bypassing technical defenses through psychological manipulation.

3.2. Supply Chain Attacks

When discussing security risks related to Internet-of-Things (IoT) products, a predominant focus usually falls on vulnerabilities in software which might reveal data or enable unauthorized access. A lesser-explored topic in the field is the integrity of the hardware itself, which can be compromised by a variety of means. In the case of IoT devices placed in homes or offices, attackers often have easy physical access to the sensors or controllers for these connections. Alternatively, it is possible to carry out a large-scale attack against a component in an IoT device's supply chain. This text delves into some of the ways an attacker may, after completing a thorough reverse engineering, poison the supply chains of consumer products which have low margins, high volume, and often stable design such as IoT devices. Such attacks can lead to the introduction of counterfeit components, which might compromise the integrity and functionality of these devices. By exploiting vulnerabilities in the supply chain, attackers can manipulate the manufacturing process to embed malicious code or hardware backdoors, posing significant risks to end-users and organizations alike [47].

The IoT ecosystem involves a complex interplay between suppliers and devices, with multiple levels of interaction. Figure 9 illustrates this through an example of two devices sourced from two distinct suppliers. While supply chains can extend across multiple tiers due to the involvement of different manufacturers for individual components, the discussion here focuses on the direct supplier of standalone devices for simplicity. Several key interactions can arise in such a setup:

1. **Device-Supplier Interactions:** These represent standard buyer-supplier relationships where devices are acquired under service contracts that include maintenance, upgrades, and security patches. Suppliers must meet the security and support requirements stipulated in these agreements.

2. **Supplier-Supplier Interactions:** Although suppliers may appear distinct on the surface, they can have shared connections at the back end, such as through mergers or acquisitions. This consolidation allows common entities to exercise greater control over the IoT supply chain, increasing the risk of coordinated attacks via backdoor channels or advanced persistent threats.

3. **Device-Device Interactions:** These arise from the interconnectivity of IoT devices, enabling them to collaborate to deliver desired functionalities. However, such interactions can also propagate supply chain risks from one device to another, bypassing the constraints of their individual supply chains.

These interactions collectively underscore the multifaceted security challenges within IoT networks.

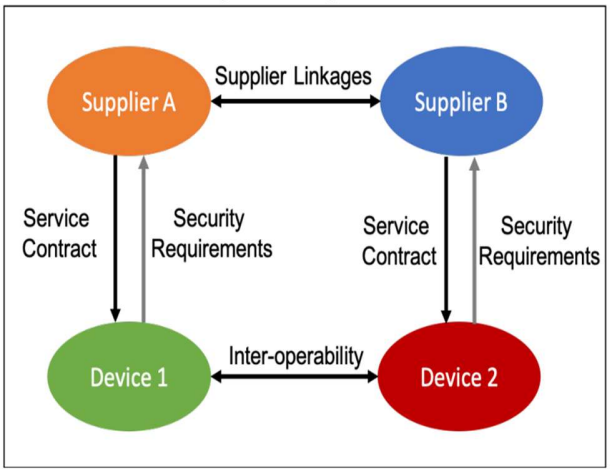

Figure 9. Key interactions between different players in the supply chain ecosystem of the IoT

Supply chain attacks essentially compromise a device at the point of its making instead of later on as part of a customer-initiated setup process. Given that most security organizations for consumer devices are oriented around attacks subsequently to their purchase, the only attack vectors considered by firms in their initial product designs are those which can be sourced back to the consumer. As with software and the advent of anti-virus/anti-malware utilities, IoT product makers will have to shift focus from this post-purchase view of attacks to an assumption of already-compromised commodities where they may form their security protocols. The IoT hardware supply chain is

complex and variable which offers an attacker a good opportunity to escape detection. There is massive diversity in hardware components used by IoT devices, they are distributed through a numerous number of suppliers, and are incorporated into products at a variety of density. This variety and huge number of actors also makes enforcing consistency in security practices across the supply chain problematic [48]. The currently mostly unconsidered threat vector of supply-elicited attacks is real, demonstrated when consumer access goods contain unanticipated vulnerabilities. Far from theoretical, these attacks have demonstrably both stolen gigabytes of sensitive data and resulted in millions of dollars worth of hardware failures. More broadly impacting have been supply chain attacks posing dangerous operational disruptions. Effective risk assessment monitoring along the IoT hardware supply chain would require a collaborative effort involving both the IoT manufacturers and their material providers. Until supply chain integrity can be assured, all other efforts at protecting the security of IoT hardware are of limited utility [49].

Figure 10 offers a more detailed representation of the interaction between the supply chain and the physical IoT network. Within this ecosystem, a component graph outlines the connectivity among devices that constitute the IoT system. Each device operates with its own distinct supply chain, yet these supply chains can be interconnected, not only through external partnerships but also through the physical links between devices in the IoT network. This interconnectivity means that risks are shared and can propagate across the network—your risk becomes mine, and mine becomes yours. Consequently, analyzing supply chain risks in IoT systems becomes highly complex due to this reciprocal nature of risk.

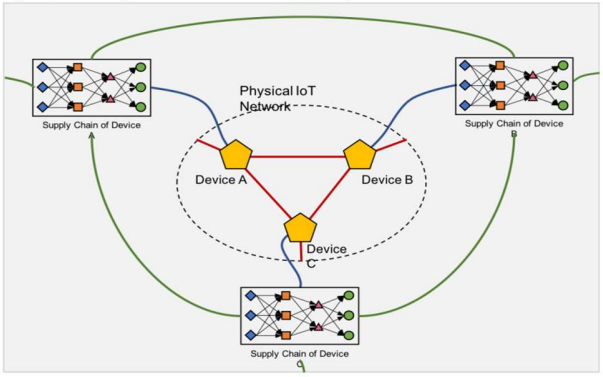

Figure 10. Mapping of IoT and the underlying supply chain networks.

3.3. Artificial Intelligence in Hardware Attacks

In the escalating arms race that characterizes hardware security in general and the Internet-of-Things (IoT) in particular, Artificial Intelligence provides a dual-edge sword. On one end, it is a potent tool for security professionals, enabling them to enhance devices, systems and networks of things with better and more efficient security measures. On the other hand, Artificial Intelligence opens the door to more powerful and sophisticated attacks, allowing attackers to fully automate and optimize the multistep process of differently attacking hardware attacks [50]. This duality of AI in hardware security necessitates a comprehensive understanding of its implications, as the same algorithms that bolster defenses can also empower adversaries. Consequently, researchers and industry leaders must prioritize developing AI-driven solutions that not only protect devices but also anticipate and counter potential threats effectively. The execution side of the attacks can be fully automated, significantly facilitating responsible vs traditional test and tuning efforts. Machine learning can help in revealing potential vulnerabilities on the target device or network, and reinforcement learning can advance strategies to optimally exploit those flaws, i.e., equip botnets with more evolved attack swarm that targets optimal devices at optimal times and locations [51]. These new attack means are expected not only to prevail traditional IoT hardware challenges and common practices for unleashing them, rapidly become a disastrous threat unless novel and adaptive security measures are implemented to counter them effectively [52].

Artificial Intelligence has already become widely adopted by technology companies, and it is now conceivable that large-scale botnets and other malicious networks of the things as well are using AI-driven attacks. To draw the big picture and to ground all arguments, five plausible scenarios describe the potential of AI exploitation in the context of hardware attacks and illustrate their implications [53]. The final part is a thoughtful mention of the exigency for adaptive and AI-aware security measures in order to keep IoT hardware that well-guard devices, systems, and networks of the things are safe and reliable. This necessity is underscored by the rapidly evolving landscape of IoT threats, which increasingly leverage sophisticated algorithms to exploit vulnerabilities in hardware. As such, organizations must implement

robust AI-driven defenses that not only respond to current threats but also anticipate future ones. Ultimately, a meaningful and effective response to the emerging AI-driven threats will necessitate a combination of hardware expertise and security insights and collaborative effort between technology companies and the online safety community, as well as with researchers and policymakers, so as to develop agile hardware and legal frameworks respectably [54].
Machine learning (ML) is not a new concept; its origins date back to the 1970s with the introduction of early algorithms . ML focuses on extracting features from data to address predictive tasks such as forecasting, anomaly detection, spam filtering, and credit risk assessment. The primary objective of ML is to make predictions based on input data. Data serves as the foundation of every ML system. For instance, to determine whether an email is spam, the system must be trained with examples of spam messages the more diverse the training data, the more accurate the predictions. Input data in ML is generally categorized into training and testing datasets. The training data is used to develop the ML model, and once the model demonstrates satisfactory prediction accuracy, the test data is employed to evaluate its performance.
The key components of ML include tasks, models, and features. Tasks represent the problems that ML aims to solve, with most models tailored to address a limited set of tasks. Models are the outputs of ML systems, trained using sample data to process new data for predictions. Features are critical as they represent characteristics of the input data, facilitating the identification of patterns between inputs and outputs. Algorithms play a vital role in solving learning tasks. As Flach explains, machine learning is the art of selecting the right features and developing suitable models to solve specific problems effectively.
Machine learning tasks are generally categorized into four types: Supervised Learning, Unsupervised Learning, Semi-supervised Learning, and Reinforcement Learning, as shown in Figure 11.

Supervised Learning involves training an algorithm using a labeled dataset, where patterns are learned to perform prediction or classification tasks. The training data is either pre-categorized or numerical, and the tasks are divided into Classification and Regression techniques. In contrast, **Unsupervised Learning** operates on unlabeled data, where algorithms analyze similarities among input elements to extract meaningful features and infer potential output labels.

Semi-supervised Learning combines aspects of both supervised and unsupervised learning, extending elements of one type with characteristics of the other to enhance learning capabilities. Lastly,

Reinforcement Learning is a method where an agent interacts with its environment through trial and error, receiving feedback in the form of rewards based on its actions. The primary objective of reinforcement learning is to enable the agent to learn optimal actions that maximize the cumulative reward through its experiences.

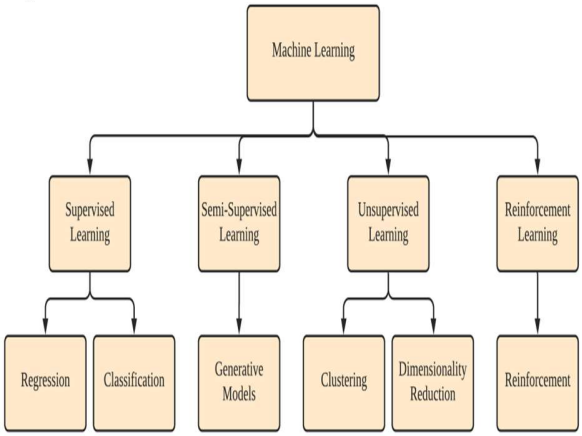

Figure 11. Machine Learning Task Categories

The attack surface of an AI system refers to the complete range of vulnerabilities that the AI model may encounter during its training and testing phases. It can also be understood as the set of all potential inputs that an adversary might exploit to compromise the system. As illustrated in Figure 12, the attack surface can be conceptualized through a generalized data processing pipeline, consisting of the training and test input data or objects, the learning algorithm or model, and the output data. During the testing phase, the machine learning model processes input features to generate class probabilities, which are then relayed to an external system for further action. Adversaries may exploit this system by manipulating the training data, compromising the learning model, or altering the class probabilities.

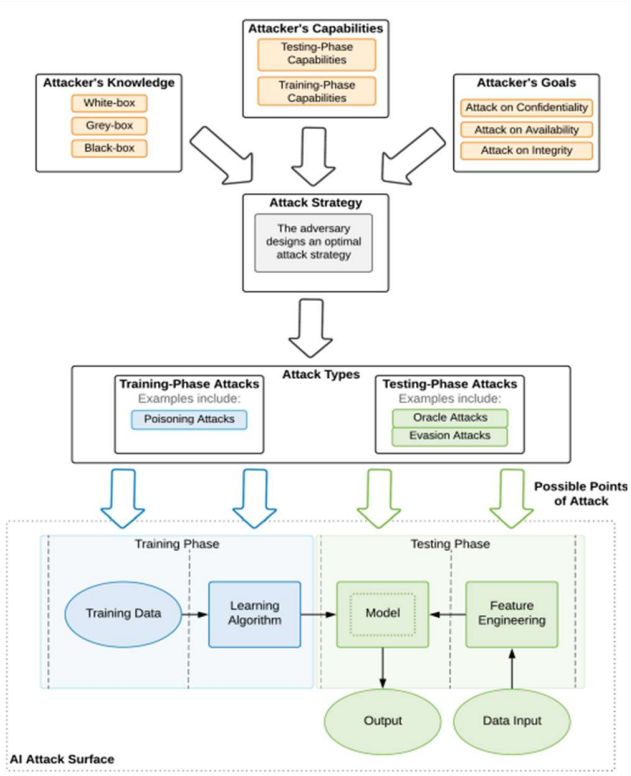

Figure 12. Proposed Framework for analysis of adversarial attacks against AI models

4. Case Studies

From a range of low-cost surveillance gadgets to pricey data analytics SaaS services in the cloud, smart home devices have revolutionized our everyday life. While raising living standards and offering innovative services to enhance life's comfort, smart home initiatives have got many people worried about potential security and privacy problems. With a significant drive towards device and network standardization facilitated by 5G network infrastructures and the ongoing massive deployment of IoT devices, the attack surface available to adversaries is rapidly expanding multifaceted devices and multifarious wireless technologies [8]. The design and manufacturing process of resource-constrained IoT devices is usually rushed to satisfy the short time to market requirements, leading to vulnerable devices that rehearse in most cases the same design and security-related issues, e.g. shared default keys, unencrypted communication, or hard-coded passwords. Moreover, IoT devices are predicting extended life cycles up to decades, during which updates stop being released after a few years. This situation magnifies the surface for numerous trivial and effective attacks. Without better security practices being implemented, the security enterprise IoT devices landscape is destined to worsen. This is particularly concerning as the proliferation of connected devices continues to accelerate, leaving a vast attack surface for potential adversaries. Manufacturers and developers must prioritize security in the design and deployment phases to ensure that vulnerabilities are addressed before devices reach consumers.

Evolution of IoT ecosystems and the arising security challenges are briefly covered. Their practical implications for end-users, device manufacturers, network vendors, and service providers are then discussed. A range of attack surfaces, from pre-installation to post-deployment, that could be explored and exploited by adversaries are investigated. Finally, a series of Hardware Trojans as attack vectors resulting from exposed internal buses and debug interfaces allegations are studied more deeply by recapping recent case studies of real-world incidents. With IoT systems steadily advancing into critical applications, from smart home environments to urban infrastructures and Industry 4.0, a worrisome trend of largely preventable security oversights is observed [55]. Given the devastating impact that cyber-attacks can have on health and safety, industrial applications, critical infrastructures, financial stability, and societal functions, now more than ever, it's imperative to continuously assess, improve, and ensure trustworthiness on newly developed and deployed connected devices.

4.1. Stuxnet

When it was first discovered in 2010, the Stuxnet worm served as a seminal case study at the intersection of cyber warfare and Internet-of-Things hardware security. The world read in rapt amazement and horror as a sophisticated piece of malicious software infiltrated Iran's Natanz enrichment facility and caused physical damage to its centrifuges. Since then, Stuxnet has taken on an almost mythical aspect, alternating between case-study, boogeyman, and tactical primer for "offensive control theory" that continues to reverberate both across the popular conscience and the international policy landscape. At its core, Stuxnet represented an unprecedented attack on industrial control systems, relying on a chain of unknown vulnerabilities along with established techniques of covert-ops tradecraft lifted directly from

the republications. Moreover, Stuxnet carried with it an array of mechanical, electrical, and biological safety limits, beautifully vivid in their operational constraints but difficult to uncover without a top-to-bottom view of the actual target and mechanisms that could be exploited by attackers seeking to disrupt critical infrastructure. This highlighted the vulnerabilities inherent in IoT devices, where interconnected systems could be manipulated to cause significant damage. As the first known cyber-weapon, Stuxnet not only set a precedent for future attacks on hardware security but also raised crucial questions regarding the protection of IoT networks against similar threats [56].

Recent research has shown that payloads specifically aimed at overvoltage conditions are effectively in broad use across significant infrastructures, and quite illuminatingly Stuxnet itself contained a crude mechanism for their detection [57]. There are also well be extend-stop-attack and slow-stop-attack codes containing tuples for frequency and duration, but the actual functionality of these are as yet not known. For all these reasons, the robustness of Stuxnet as an attack should be strongly emphasized, and the case, rather than simply an illustration of what can go wrong, should be taken as representative of the difficulties in attacking or defending machines that due to their complexity, are still only partially understood by their operators or builders. At the time of its development, a decade ago, the acquisition of a machine by a dedicated adversary for the purposes of designing an analog of Stuxnet by an analogous process of cryptanalysis would have presented a formidable, though conceivably not insurmountable challenge. The example of Stuxnet, though certainly exceptional, does provide significant lessons for both attackers and defenders and further underlines the ongoing evolution of threats in the context of hardware security, especially as applied to the fungal architectures of systems and the more general ecosystem [58].

4.2. Mirai Botnet

The threat posed by Mirai peaked in September 2016 with a DDoS attack against partner site which at its peak reached traffic of 623Gbit/s. The traffic initiated by Mirai compromised peers reached 1.1Tbit/s and remained at 500Mbit/s high-bandwidth traffic long after the other attacks had stopped. Network traffic during other events indicated Mirai causing Command and Control (C2) servers to go offline, preventing reflection partners from being instructed to attack the target as a form of ‘clean-up’. This was a rarer and more harmful strategy, resulting in total downtime of five hours for the target. IoT devices used in this scenario were observed to malfunction after being instructed to carry out tasks. The functions of one device were delayed by a matter of milliseconds, which was enough to cause it to crash, reboot, and no longer perform the task. This vulnerability was exploited by the Mirai botnet, which leveraged the compromised devices to execute coordinated attacks, overwhelming targeted servers with traffic and rendering them inoperable. As a result, the botnet was able to launch Distributed Denial of Service (DDoS) attacks on a massive scale. By exploiting the inherent weaknesses in IoT devices, the Mirai botnet exemplified the critical need for improved security measures in the design and implementation of connected hardware.

By plugging these devices into monitoring network hardware, large spikes in network bandwidth (tens of Gbit/s) were observed leaving the device, with no correlation to their intended actions. reported that the event was the first ever terabit per second DDoS attack, however the traffic received by was closer to 80Mbit/s from a 24-hour perspective and barely reached 140Mbit/s from an hourly perspective [59]. There are two separate traffic graph anomalies unrelated to the main attack where different groups of compromised devices spastically (and pointlessly) burst every few hours. Ultimately, the device malfunctions caused by Mirai resulted in an inability to reach the target. This created significant vulnerabilities that were exploited by attackers, leading to widespread disruption of services.

5. Recommendations for Enhancing IoT Hardware Security

The following practical recommendations elaborate on ways to bolstering security in IoT hardware following the identification of current and emerging threats as explained previously [43]. First, to bolster the security stance of IoT hardware solutions against emerging and future threats, the process of designing the hardware ecosystem must be secure. Security must be integrated from the inception of an idea up to the production or maintenance of the product. Secure design is thus an approach for the development of security measures at the initial stage

of development and through all the design stages. Secure devices and systems are significantly more difficult to exploit than those that are not secure. Moreover, a strategy is proposed that can be exploited through all the stages of the supply chain, since each of the stages is vulnerable. Such an approach has been proven to be very effective in defending products, but there are still missing tools and best practices that could be applied in this strategy. To avoid awareness of possible vulnerabilities, organizations that create potential weaknesses must be procured as trusted partners. It is essential for these organizations to implement robust security measures and regularly undergo audits to identify and mitigate risks before they can be exploited [60].

Secure devices, as commercially available alternatives, must be used. More transparent procedures must be applied, and audits must be implemented on a frequent basis. Both the benefits and shortcomings of this approach are discussed, and key principles that have been derived from these considerations are presented. The first principle is to implement a robust authentication mechanism for devices, ensuring that only authorized users can access and control IoT devices. Furthermore, regular software updates and patches are essential to mitigate vulnerabilities that may arise over time. These updates should be implemented not only for the operating system but also for the various applications that run on IoT devices. Additionally, manufacturers should adopt a proactive approach by integrating security features during the design phase, ensuring that devices are equipped to handle potential threats from the outset [11].

Second, to create a more fertile infrastructure for these devices, it is necessary for actors to coherently collaborate. Optoelectronics industry stakeholders were divided into three groups: manufacturing, and research and education, and their engagement in security approaches has been actively surveyed. The outcomes reveal inconsistencies between stakeholders, e.g. the perception of security and the level of awareness, which hinder policy planning but may be easily addressed by developing standards and best practices. Such solutions have the potential to enhance the effectiveness of the suggested security measures and tools. Third, some AI-accelerated defensive methods, which may efficiently improve the proposed measures, are presented. These methods leverage machine learning algorithms to detect anomalies in device behavior, thereby fortifying the overall security posture of IoT systems. This proactive approach not only identifies potential threats in real-time but also allows for adaptive responses to emerging vulnerabilities [61].

5.1. Secure Hardware Design

Secure hardware design is the cornerstone of an IoT device secure implementation and a strong first line of defense against hacks and cyber-attacks on IoT products. Many of the secure design principles are device design methodology considering throughout the device and integrated circuit design or selection rather than software implementations post fabrication [19]. Encrypted elements, especially those in areas of critical operation, cannot be reverse engineered hence secure software should never be run from decrypted memory, XOR-ing encrypted instructions and keys with geometry pattern PRNG, on-the-fly decryption or encrypting individual instructions post place and route are common methods for this implementation [62]. Normally executed for data, not normal CPU instructions as in other designs, the trusted computing base consists of encrypted boot ROM and SRAM controlled by dedicated ROM based state machine allows system bring up, self checking and run-time cryptography, so all code is run out of encrypted memory using a block cipher keyed once on power up. In recent years, hardware vulnerabilities have become a primary concern for IoT devices rather than software bugs, because a number of successful cyber-attacks on IoT devices utilize hardware vulnerabilities. The findings show that hardware threats outpace the software threats at least 2 years possibly due to the commoditization of the system on chip industry. Hardware-rooted threats are the root causes of ~70% of the product vulnerabilities and create pervasive vulnerabilities in various aspect of product functions compared with only ~30% of threats of software/content attack vectors [63]. This motivation is contrary to the common belief that hardware threats are much less nascent compared to the software threats. In summary, it is convinced that the industry needs to pay close attention to emerging hardware security challenges and develop effective strategies and technologies to mitigate hardware vulnerabilities. To achieve this, a comprehensive approach should be adopted that includes enhanced encryption methods, secure boot processes, and continuous monitoring for potential threats. By prioritizing secure hardware

design, manufacturers can significantly reduce the risk of exploitation and ensure the integrity of IoT devices. This approach not only enhances the device's ability to withstand attacks but also fosters user trust in the technology. Implementing features such as secure boot, hardware-based encryption, and tamper detection mechanisms are essential steps in this process [64].

5.2. Supply Chain Security

Supply Chain Security The Internet of Things (IoT) has never been more prevalent; IoT hardware sales are skyrocketing and are expected to reach over 1 trillion by 2025. Many IoT devices have access to private, personal, or even classified information. The importance of indicating that IoT remains secure aside, lack of awareness exists for a specific, understudied discipline. Regulatory focus on network rather than hardware security. This shift often leads to inadequate measures being taken to protect the devices themselves, which are increasingly vulnerable to attacks. As the IoT ecosystem expands, it becomes crucial to address the security of hardware components within the supply chain [46]. However, as IoT hardware becomes more prevalent in everyday objects, its security is pertinent. More notably, there is a mist of mystery surrounding hardware. Design and process are closely guarded due to economic reasons. Keeping hardware aspects secret while fostering an upward trend in its use creates a fertile ground for undetected vulnerabilities. Novel hardware security threats emerge through evolving exfiltration techniques and improved capabilities of adversaries [47].

As a general principle, IoT devices are designed to be inconspicuous. However, this concept perversely extends to the hardware as well. Publicly available knowledge for the hardware is either extremely technical or simplified marketing material. The ecosystem aspect of IoT allows for devices to be sold without chip-level data - only certain functionality needs be determined. This lack of transparency in the supply chain can lead to vulnerabilities, as malicious entities may exploit these gaps to introduce compromised components. Ensuring robust supply chain security is crucial for maintaining the integrity of IoT devices and protecting user data [65]. Hardware supply chain security is more complex than its software counterpart. The induction of a vulnerability at any step of creation of a chip can be imperceptible until a later step. For example, a trojan chip that is created in the design step can manifest a vulnerability during the testing step. Both design and fabrication steps can change hands multiple times, complicating efforts to monitor the entirety of a single chip creation. Each hardware manufacturer can use a variety of other manufacturers to create different components. Each component can be manipulated separately. There is no easy analog to checksums or signatures that software have to determine the authenticity of a chip. Manufacturers are not incentivized to provide the capability to detect malicious alteration. There is a high vertical silo between most IC manufacturers and those that purchase ICs in bulk [66].

The security of the former is not shared with the latter. One part of greater supply chain security is proving the integrity of a device from creation to reception. However, only forthcoming companies are required to document this process. Best practice recommendation is to use this vacuum in law to advantage. The IoT device manufacturer, instead of the hardware, is rarely inspected for supply chain security. Whether it be the adherence to a robust set of security guidelines or the criterion that its components are bought from secure sources, companies can copiously evaluate the security of their providers [67][68]. Classic trend in security is for a closed source to become open source. Optimization of coordination and transparency is a far better path for security. Both espionage and tampering are infinitesimally harder when work is public. Government investment in more than unidirectional programs. Allowing greater introspection towards hostile governments could form a more balanced and reciprocal mindset toward weaponized chips. Because IoT hardware security is a particularly nebulous area, the fostering of a security-aware culture across the continuum of the supply chain is promulgated. This includes educating all stakeholders about potential vulnerabilities and encouraging proactive measures to mitigate risks. Implementing rigorous vetting processes for suppliers and ensuring that security best practices are integrated into every stage of the product lifecycle are essential steps in enhancing supply chain security [69].

5.3. Regular Hardware Audits

It is vital to audit the hardware periodically as there could be security issues that could have been

overlooked during the initial hardware review or new types of vulnerabilities that have emerged since [70]. The audit should ideally follow the structured processes outlined in this memo and a record of the audit and changes should be maintained. The audit should also evaluate the security of the overall IoT device infrastructure. Additionally, the audits should encompass detecting and mitigating the devices that pose a security risk to the organization's network and that the IoT devices hardware and physical integrity are protected. This includes regular checks for firmware vulnerabilities, ensuring that all software is up to date, and verifying that access controls are effectively implemented. Furthermore, organizations should establish protocols for addressing any identified weaknesses promptly and efficiently [71].
Hardware audit reviews of IoT devices for vulnerabilities and proper usage. IoT devices are increasingly deployed in businesses, homes, and industrial environments. It is important to periodically review the security posture of IoT devices similar to the way that a network or software would be reviewed for compliance and potential issues. It is likely that an IoT device would be deployed indefinitely and a periodic hardware audit should evaluate the security posture and the devices for compliance. Hardware audit also allows the early detection any security issues related to new IoT devices before those issues become widespread [18]. It is recommended that hardware reviews are integrated into the standard audits framework for other devices. Here are some of the formal hardware auditing processes that can be followed: Engage with various teams and review available documentation, Identify a security baseline, Evaluate the physical hardware for compliance with the baseline, Make changes if the device is found to be a compliance risk, and Maintain ongoing review and follow-up with the teams involved in changing each device. While having a review it is best practice to notify the device owner and attempt to provide recommendations for improvement, and, if any changes are made, attempt to document those changes centrally. It is also recommended that a hardware audit include a cross-functional team, including physical security, network, compliance, and systems teams. This collaborative approach ensures that all relevant perspectives are considered, leading to a more comprehensive assessment of potential vulnerabilities. Furthermore, regular audits can help identify not only existing issues but also areas for future improvement [72]

5.4. Collaboration and Standards

Mitigating the multifaceted threats to Internet-of-Things (IoT) hardware security necessitate collaboration across diverse sectors comprising manufacturers, regulatory bodies, and specialists in cybersecurity. A coordinated frontline approach is required to ensure the seamless integration of security practices throughout the supply chain; however, the current polarization in understanding IoT security risks hinders the realization of unified tangible countermeasures [73]. Given the unprecedented expansion of the IoT landscape, there is common agreement on the timeliness of manufacturer-agnostic industry standards for IoT hardware security. This is particularly crucial for ensuring interoperability and enhancing the trustworthiness of devices across different platforms. By fostering collaboration among manufacturers, regulators, and industry stakeholders, we can create a robust framework that not only addresses current vulnerabilities but also anticipates future threats in the IoT ecosystem. This collaborative approach will facilitate the development of standardized security protocols that can be universally adopted, thereby enhancing the overall resilience of IoT devices against emerging threats.As of today, emphases on IoT security largely mirror the distinct supply chain postures of stakeholders concerning their scope of responsibilities. In addressing IoT hardware security threats, security standard bodies are crucial to establish a more coherent playing ground among the different sectors involved in the IoT value chain [18]. Ensuring compliance and consistency regarding practices adopted by vendors and original equipment manufacturers (OEMs) can facilitate security best practices in IoT device development and manufacturing. Existing initiatives striving to unify the third-party cybersecurity caste across an industry-wide standard framework are viewed as essential enablers of security scaling in the IoT hardware domain [74]. A multilateral coalescence regarding security criticalities across all IoT segments, involving shared knowledge and resource transfer from OEMs, is believed to better leverage the creativity and innovation in the cybersecurity community. Given the current disjointed legislative status, several challenges underline the massive adoption and commitment of security standards prevailing a diversified IoT

hardware market. Advocates stress the need for public-private partnerships in order to embody broader standards underlying the foundational aim of limiting emerging risks associated with the fast-evolving IoT hardware vulnerabilities [75].

5.5. Use of AI for Defense

Artificial Intelligence, in some studies referred to as AI, is turning out to be commonsensical as a defensive mechanism for the Internet-of-Things. In this context, AI may be used on the one hand to detect abnormal hardware behaviors - in which case AI serves as a defense mechanism, and on the other hand, AI may be used to hack hardware, which corresponds to an attack mechanism. AI offers versatile defense mechanisms for monitoring digitized and system-level hardware operation so that potential threats are detected in real-time [76]. A significant advantage is that machine behavior/learning (MB/L) algorithms in combination with dedicated Artificial Intelligence can evolve over time and thereby adapt to new and currently unknown attack techniques. This capability allows for proactive measures to be implemented, significantly enhancing the resilience of IoT systems against sophisticated breaches.

By integrating AI-driven analytics, security protocols can be continuously updated and adapted to counter emerging threats, thereby safeguarding critical data and ensuring the integrity of connected devices. This proactive approach not only enhances the resilience of IoT systems but also allows for real-time threat detection and response. Furthermore, AI can facilitate the identification of unusual behavior patterns, which may indicate a potential security breach, enabling swift remedial actions. This puts attackers at a disadvantage in that their novel strategies could rapidly go out of date. Consequently, organizations can leverage artificial intelligence to enhance their security measures, adapting to emerging threats in real-time. Although most attacks are aimed at software, AI can also be relevant for detecting hardware vulnerabilities or for hacking hardware. In particular, the implementation of AI in automation aims at threat (i) detection processes that are constantly getting smarter; (ii) response processes that have reached near-human potential in streamlining all security operations. In line with the hacker's perspective, it is generally assumed that AI attackers will be at least as competent in finding loopholes in existing architectures as developers of AI defense mechanisms. This requires the collaboration between the AI community and hardware security experts. By leveraging advanced algorithms and data analytics, they can identify vulnerabilities and devise proactive measures to safeguard IoT devices from potential threats [77].

However, AI defensive (as well as AI attack) approaches will need to be in reach of the broader community. Hence, companies working in hardware should support the development of open-source AI-driven defenses; alternatively, the generation of common AI attack/defense toolboxes should be encouraged. It is anticipated that the generation of AI attack/defense networks will be of specific interest to academia since the possibilities for obtaining valuable information will increase beyond the strict hardware field [78]. This will not only enhance the understanding of potential vulnerabilities in IoT devices but also foster the development of robust defense mechanisms that can anticipate and counteract emerging threats. Partnerships between academia and industry in AI-related subjects are expected. Yet, implementation of AI has its challenges, considering that (i) not all respective assets are readily available and (ii) there is a tremendous risk of getting overwhelmed by a substantial amount of false positives that are often biased. Therefore, it is essential to press for further AI research in the field, and collective efforts from industry, governments, as well as academia and other stakeholders, are required to foster AI-driven threats to outperform emerging attack strategies [79].

6. Future Directions

The exponential growth of IoT devices would result in a surge in cyber threats concerning several applications. The increasing number of connected devices set up in a network increases its complexity and results in potential violation because of numerous vulnerabilities that are hard to find, make problematic to protect from hacking, and more threatens from being violated. This complexity not only heightens the risk of cyberattacks but also complicates the development of effective security measures. To address these emerging threats, it is essential to explore innovative security frameworks that can adapt to the ever-evolving landscape of IoT devices. First the security loopholes and challenges confronted in IoT applications have been discussed. It shows how such threats motivate innovation towards techniques

where distinct cooperative schemes among emerging technologies look at IoT safety and security have to be unified for streamlining the safeguards [80]. It elucidates and represents a few of the cooperative setups that can be studied between the security framework of hardware arrangement, dangerous cyber risks, and procedures. By exploring these collaborative models, we can better understand how to enhance the resilience of IoT systems against emerging threats. Future research should focus on integrating advanced encryption techniques, developing adaptive response mechanisms, and fostering cross-industry partnerships to address the evolving landscape of IoT hardware security.

As the development of technology is increasing at a very high pace, it is giving rise to a large number of devices. The IoT is the principle initiative unified with the aim of combining resources through the USB. It can also be said that the IoT device is showing connections through wires and cables. Each of the devices that are thus connected in the web is known as 'IoT Device' [43]. To develop a connected world, the IoT devices are brought into play, enabling error-free and timely completion of the task – convenient availability. As the technology develops, its use can be seen from a thermometer to huge mechanizations, the IoT Technology has strengthened and broadened its wings.

As far as security is concerned, the IoT device is soundly secured. It is a systematic security champion platform through the usage of the appropriate platform. The Application Programming Interface (API) makes the device secure at an easy pace and provides explicit security as well. This approach can enhance the security of IoT devices across various sectors, ensuring that both consumer and industrial applications are safeguarded against potential vulnerabilities [81]. Considering all these, this methodology secures the job and minimizes the malicious attempts to connive to the device. With this methodology, the variety of applications may be used effectively and in a sensible way.

7. Conclusion

In conclusion, it is the age of IoT, as evolving technology trends and consumer demand continue to pave the way for a plethora of new devices and services. However, this also means that a more extensive IoT hardware security framework must be established urgently. Many security risks and flaws exist within the IoT hardware sector, either inherently or as a result of its volatile operating environment. Case studies show just how faulty implementation can result in very vulnerable, technically "secure" devices. This highlights the critical need for robust security measures in the design and implementation phases. Without proper attention to these aspects, even devices that are theoretically secure can become susceptible to exploitation by malicious actors. This vulnerability highlights the critical need for robust security measures to be integrated into the design and deployment of IoT devices. As technology continues to evolve, so too must our strategies for safeguarding these systems against emerging threats.

It is essential to increase the focus on IoT hardware security. Devices within an IoT ecosystem can be safeguarded through "secure-by-design" principles like those integrated into the regulations as part of the European Electronic Communications Code in 2018. Supply chain integrity ensures that a core aspect of hardware security cannot be bypassed or interfered with. Codes of Conduct will drive both makers and operators towards proactively secure hardware requirements. Although future secure hardware requirements for Makers and Operators are not yet finalized or fully defined, it is important that manufacturers and operators are already considering any such developments within their infrastructure. Such steps will only help to maintain and improve the consumer trust in IoT devices, and the services derived from them. This is essential in fostering a secure ecosystem that supports the growing reliance on connected technologies.

After all, consumer trust is the backbone of all successful products, no matter how innovative or disruptive they are. Or the best devices in the world would not sell if they were unsafe or untrustworthy. It is better to take proactive steps to ensure that these imaginable horizons of insecurity are also the unimaginable. There will always be emerging issues, but parties can also take proactive steps in preparation for a more secure future. So, on with the security minds! On with the encryptions! All forms of digital technology are evolving, and so must our approach to their protection. This reality is particularly pertinent in the context of the Internet-of-Things (IoT), where the proliferation of connected devices introduces unique vulnerabilities. As we have discussed throughout this work, the security of IoT hardware is paramount to safeguarding both personal and organizational data

from emerging threats. Moving forward, it is essential to adopt a proactive stance towards IoT security, incorporating robust encryption methods, regular firmware updates, and comprehensive risk assessments to mitigate potential risks.

Acknowledgment

The authors would like to thank the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia for the assistance.

References

[1] Y. B. Zikria, R. Ali, M. K. Afzal, and S. W. Kim, "Next-generation internet of things (iot): Opportunities, challenges, and solutions," Sensors, 2021. mdpi.com

[2] R. A. Khalil, N. Saeed, M. Masood, and Y. M. Fard, "Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications," in *Internet of Things*, 2021.

[3] K. O. M. Salih, T. A. Rashid, D. Radovanovic, and N. Bacanin, "A comprehensive survey on the Internet of Things with the industrial marketplace," Sensors, 2022. mdpi.com

[4] P. Francik, M. Poplawski, S. N. G. Gourisetti, and P. O'Connell, "A Cybersecurity Threat Profile for a Connected Lighting System," 2022. osti.gov

[5] O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, "IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience," Asian Journal of ..., 2023. ssrn.com

[6] S. Nižetić, P. Šolić, D. L. I. Gonzalez-De, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," Journal of Cleaner Production, 2020. nih.gov

[7] W. Hu, C. H. Chang, A. Sengupta, and S. Bhunia, "An overview of hardware security and trust: Threats, countermeasures, and design tools," in *… on Computer-Aided …*, 2020. ntu.edu.sg

[8] A. Hamza, H. Habibi Gharakheili, and V. Sivaraman, "IoT Network Security: Requirements, Threats, and Countermeasures," 2020.

[9] X. Feng, X. Zhu, Q. L. Han, and W. Zhou, "Detecting vulnerability on IoT device firmware: A survey," IEEE/CAA Journal of ..., 2022. ieee-jas.net

[10] A. McGowan, S. Sittig, and T. Andel, "Medical internet of things: a survey of the current threat and vulnerability landscape," 2021. hawaii.edu

[11] A. Jurcut, T. Niculcea, P. Ranaweera, and N. A. Le-Khac, "Security considerations for Internet of Things: A survey," SN Computer Science, 2020.

[12] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, "Internet of things applications: opportunities and threats," *Wireless Personal …*, Springer, 2022. springer.com

[13] O. Hosam, R. Abousamra, and M. Hassouna, "Security analysis and planning for enterprise networks: Incorporating modern security design principles," in … and Design Principles …, 2024. researchgate.net

[14] C. Xenofontos, I. Zografopoulos, "Consumer, commercial, and industrial IoT (in) security: Attack taxonomy and case studies," IEEE Internet of Things Journal, 2021.

[15] A. Martikkala, J. David, A. Lobov, M. Lanz et al., "Trends for low-cost and open-source IoT solutions development for industry 4.0," Procedia Manufacturing, 2021. sciencedirect.com

[16] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT security," in *IoT security: advances in …*, 2020, Wiley Online Library. researchgate.net

[17] S. Tedeschi, J. Mehnen, N. Tapoglou, and R. Roy, "Secure IoT devices for the maintenance of machine tools," 2017.

[18] [18] J. M Blythe, N. Sombatruang, and S. Johnson, "What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?," 2019. osf.io

[19] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, and M. Ziörjen, "Landscape of IoT security," Computer Science, Elsevier, 2022. sciencedirect.com

[20] J. Kinney, "Analyzing Insider Risk Threat to the Internet of Things (IoT)," 2023. osti.gov

[21] [21] A. Muñoz, "Cracking the Core: Hardware Vulnerabilities in Android Devices Unveiled," Electronics, 2024. mdpi.com

[22] R. Ramadan, "Internet of things (iot) security vulnerabilities: A review," PLOMS AI, 2022. plomscience.com

[23] R. F. Olanrewaju, B. U. I. Khan, M. L. M. Kiah, and N. A. Abdullah, "Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT," Electronics, 2022. mdpi.com

[24] G. Palihawadana, "Silent Breaches: Exploring Emerging Threats and Defenses in Side Channel Attacks," researchgate.net, . researchgate.net

[25] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for IC chip level hardware security," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2021. ieee.org

[26] A. Hassan, N. Nizam-Uddin, A. Quddus, and S. R. Hassan, "Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of …," 2024. researchgate.net

[27] P. Anand, Y. Singh, A. Selwal, M. Alazab, and S. Tanwar, "IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges," IEEE, 2020. ieee.org

[28] M. J. Kannwischer, P. Pessl, and R. Primas, "Single-trace attacks on keccak," Cryptology ePrint Archive, 2020. iacr.org

[29] S. H. Newman, "Decentralization Cheapens Corruptive Majority Attacks," arXiv preprint arXiv:2310.01546, 2023.

[30] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, and P. K. Singh, "Internet of things: Evolution, concerns and security challenges," Sensors, 2021. mdpi.com

[31] R. Awadallah, A. Samsudin, and J. S. Teh, "An integrated architecture for maintaining security in cloud computing based on blockchain," IEEE Access, 2021. ieee.org

[32] J. Wang, Y. Liu, P. Li, Z. Lin, and S. Sindakis, "Overview of data quality: Examining the dimensions, antecedents, and

impacts of data quality," Journal of the Knowledge, 2024. springer.com
[33] D. G. S. Pivoto, L. F. F. De Almeida, R. da Rosa Righi, "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review," Manufacturing Systems, 2021, Elsevier. unizar.es
[34] S. Akter, K. Khalil, and M. Bayoumi, "A survey on hardware security: Current trends and challenges," IEEE Access, 2023. ieee.org
[35] S. Maragkou and A. Jantsch, "Information Flow Tracking Methods for Protecting Cyber-Physical Systems against Hardware Trojans - a Survey," 2022.
[36] Z. Pan and P. Mishra, "Automated test generation for hardware trojan detection using reinforcement learning," in Proceedings of the 26th Asia and South Pacific Design, 2021. acm.org
[37] K. Hameed, S. Garg, M. Bilal Amin, and B. Kang, "Towards a Formal Modelling, Analysis, and Verification of a Clone Node Attack Detection Scheme in the Internet of Things," 2021.
[38] M. Adam, M. Hammoudeh, and R. Alrawashdeh, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," IEEE, 2024. ieee.org
[39] J. Blümke and H. J. Hof, "Authentic batteries: a concept for a battery pass based on PUF-enabled certificates," in *SECURWARE 2022: The Sixteenth*, 2022. researchgate.net
[40] J. Kirkland, R. Stoddard, B. Antonov, and N. Dragomirov, "Automated detection of crypto ransomware using machine learning and file entropy analysis," Authorea, 2024. techrxiv.org
[41] Z. Muhammad, Z. Anwar, A. R. Javed, B. Saleem, S. Abbas, "Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses," Technologies, 2023. mdpi.com
[42] S. Strba, "Internet of Things Security: Ongoing Threats and Proposed Solutions," 2018.
[43] S. Kumar Sahu and K. Mazumdar, "Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance," 2024. ncbi.nlm.nih.gov
[44] R. Ávila, R. Khoury, and R. Khoury, "Use of security logs for data leak detection: a systematic literature review," Security and ..., 2021. wiley.com
[45] D. Rupanetti and N. Kaabouch, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities," Applied Sciences, 2024. mdpi.com
[46] M. Shafiq, Z. Gu, and O. Cheikhrouhou, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," Wireless, 2022. wiley.com
[47] M. Junaid Farooq and Q. Zhu, "IoT Supply Chain Security: Overview, Challenges, and the Road Ahead," 2019.
[48] V. Hassija, V. Chamola, V. Gupta, and S. Jain, "A survey on supply chain security: Application areas, security threats, and solution architectures," in Internet of Things, 2020.
[49] K. Rauniyar, X. Wu, S. Gupta, and S. Modgil, "Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology," Industrial Management, 2023. researchgate.net
[50] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey," Ieee, 2021. ieee.org
[51] A. Oseni, N. Moustafa, H. Janicke, P. Liu et al., "Security and Privacy for Artificial Intelligence: Opportunities and Challenges," 2021.
[52] J. Clements and Y. Lao, "Hardware Trojan Attacks on Neural Networks," 2018.
[53] A. Arif, M. I. Khan, and A. R. A. Khan, "An overview of cyber threats generated by AI," International Journal of …, 2024. itscience.org
[54] N. G. Camacho, "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age," Journal of Artificial Intelligence General Science, 2024. boulibrary.com
[55] Y. Su and D. C. Ranasinghe, "Leaving Your Things Unattended is No Joke! Memory Bus Snooping and Open Debug Interface Exploits," 2022.
[56] C. Stevens, "Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet," Contemporary Security Policy, 2020. tandfonline.com
[57] K. A. Khan, M. M. Quamar, F. H. Al-Qahtani, and M. Asif, "Smart grid infrastructure and renewable energy deployment: A conceptual review of Saudi Arabia," Energy Strategy, Elsevier, 2023. sciencedirect.com
[58] M. Fahad, H. Airf, and A. Kumar, "Securing Against APTs: Advancements in Detection and Mitigation," BIN: Bulletin Of, 2023. jurnalmahasiswa.com
[59] C. Kelly, N. Pitropakis, S. McKeown, and C. Lambrinoudakis, "Testing And Hardening IoT Devices Against the Mirai Botnet," 2020.
[60] S. Tatineni, "Compliance and Audit Challenges in DevOps: A Security Perspective," DevOps-An Open Access Journal, 2024. pythonpublishingpress.com
[61] O. Salman, I. H. Elhajj, A. Chehab, "A machine learning based framework for IoT device identification and abnormal traffic detection," Transactions on ..., 2022.
[62] D. Natarajan and W. Dai, "Seal-embedded: A homomorphic encryption library for the internet of things," in *IACR Transactions on Cryptographic Hardware*, 2021. iacr.org
[63] I. Tsiokanos, J. Miskelly, C. Gu, M. O'Neill, "DTA-PUF: Dynamic timing-aware physical unclonable function for resource-constrained devices," ACM Journal on ..., 2021. qub.ac.uk
[64] A. Cirne, P. R. Sousa, and J. S. Resende, "Hardware security for Internet of Things identity assurance," in Surveys & Tutorials, 2024. researchgate.net
[65] C. Bai, M. Quayson, and J. Sarkis, "Analysis of Blockchain's enablers for improving sustainable supply chain transparency in Africa cocoa industry," Journal of Cleaner Production, 2022.
[66] E. Ozen and A. Orailoglu, "Low-cost error detection in deep neural network accelerators with linear algorithmic checksums," Journal of Electronic Testing, 2020.
[67] V. Asimakopoulos, "Cloud security and privacy," 2023. unipi.gr
[68] R. D. Thantilage, N. A. Le-Khac, and M. T. Kechadi, "Healthcare data security and privacy in Data Warehouse architectures," Informatics in Medicine, Elsevier, 2023. sciencedirect.com

[69] M. Asante, G. Epiphaniou, and C. Maple, "Distributed ledger technologies in supply chain security management: A comprehensive survey," in … Management, 2021. warwick.ac.uk
[70] Z. Maamar, E. Kajan, M. Asim, and T. Baker, "Open Challenges in Vetting the Internet-of-Things," 1970.
[71] D. Ajiga, P. A. Okeleke, S. O. Folorunsho, and C. Ezeigweneme, "Designing cybersecurity measures for enterprise software applications to protect data integrity," 2024. researchgate.net
[72] L. Hut-Mossel, K. Ahaus, G. Welker, and R. Gans, "Understanding how and why audits work in improving the quality of hospital care: A systematic realist review," PloS one, 2021. plos.org
[73] J. Chen and L. Urquhart, "'They're all about pushing the products and shiny things rather than fundamental security': Mapping socio-technical challenges in securing the smart home," 2022.
[74] T. Wallis, C. Johnston, and M. Khamis, "Interorganizational cooperation in supply chain cybersecurity: a cross-industry study of the effectiveness of the UK implementation of the NIS directive," Information and Security: An …, 2021. gla.ac.uk
[75] A. J. Apeh, A. O. Hassan, and O. O. Oyewole, "GRC strategies in modern cloud infrastructures: a review of compliance challenges," Computer Science & IT, 2023. fepbl.com
[76] M. Schmitt, "Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection," 2023.
[77] V. Ziegler, P. Schneider, H. Viswanathan, and M. Montag, "Security and Trust in the 6G Era," Ieee, 2021. ieee.org
[78] T. M. Santhi and K. Srinivasan, "Chat-GPT based learning platform for creation of different attack model signatures and development of defense algorithm for cyberattack detection," IEEE Transactions on Learning, 2024.
[79] M. Amini and Z. Bozorgasl, "A game theory method to cyber-threat information sharing in cloud computing technology," International Journal of Information System, 2023. ssrn.com
[80] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," IEEE Access, 2021. ieee.org
[81] A. Diro, N. Chilamkurti, V. D. Nguyen, and W. Heyne, "A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms," Sensors, 2021. mdpi.com
[82] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, and M. Alawida, "The internet of things security: A survey encompassing unexplored areas and new insights," Computers & …, 2022.
[83] Q. Xu, M. T. Arafin, and G. Qu, "Security of neural networks from hardware perspective: A survey and beyond," in *Proceedings of the 26th Asia and South Pacific Design*, 2021. acm.org