Review

Securing Cloud-Based Internet of Things: Challenges and Mitigations

Nivedita Singh [1] , Rajkumar Buyya [2] and Hyoungshick Kim [1,*]

1   Department of Computer Science & Engineering, Sungkyunkwan University,
     Suwon 16419, Republic of Korea; singhnivvy@g.skku.edu
2   Cloud Computing and Distributed Systems (CLOUDS) Lab, School of Computing and Information Systems,
     The University of Melbourne, Parkville, VIC 3010, Australia; rbuyya@unimelb.edu.au
*   Correspondence: hyoung@skku.edu

Abstract: The Internet of Things (IoT) has seen remarkable advancements in recent years, leading to a paradigm shift in the digital landscape. However, these technological strides have introduced new challenges, particularly in cybersecurity. IoT devices, inherently connected to the internet, are susceptible to various forms of attacks. Moreover, IoT services often handle sensitive user data, which could be exploited by malicious actors or unauthorized service providers. As IoT ecosystems expand, the convergence of traditional and cloud-based systems presents unique security threats in the absence of uniform regulations. Cloud-based IoT systems, enabled by Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) models, offer flexibility and scalability but also pose additional security risks. The intricate interaction between these systems and traditional IoT devices demands comprehensive strategies to protect data integrity and user privacy. This paper highlights the pressing security concerns associated with the widespread adoption of IoT devices and services. We propose viable solutions to bridge the existing security gaps while anticipating and preparing for future challenges. This paper provides a detailed survey of the key security challenges that IoT services are currently facing. We also suggest proactive strategies to mitigate these risks, thereby strengthening the overall security of IoT devices and services.

Keywords: cloud; security; IoT security; IoT privacy; IaaS

1. Introduction

Imagine your morning coffee starts brewing as you wake up, your thermostats adjust automatically based on the weather, and a notification pops up reminding you to take your medication. The ubiquitous Internet of Things (IoT) is weaving itself into the fabric of our daily lives, promising a seamless and convenient future. Applications range from smart homes to AI-powered medical equipment, intelligent agriculture, and advancements in the automotive industry [1]. Notably, IoT health monitoring systems have significantly improved the quality of life for the elderly and disabled, with the COVID-19 outbreak highlighting IoT's potential in health [2]. Unlike traditional IoT, which relies on localized processing and storage, cloud-based IoT utilizes external cloud infrastructure for scalability, advanced analytics, and seamless device connectivity. This shift introduces unique challenges, including reliance on third-party providers, expanded attack surfaces, and privacy risks from centralized data storage, necessitating specialized security and privacy solutions.

With every connected IoT device comes a question: are we prioritizing comfort over security? This concern becomes even more serious as we delve into the world of cloud-based IoT. This survey delves into the critical security and privacy risks emerging from

the integration of IoT devices with cloud-based services, which facilitate data processing, storage, and communication. These challenges, central to this study, highlight the need for robust strategies to safeguard IoT systems as they increasingly depend on cloud infrastructure. Traditional IoT systems come with inherent limitations, particularly in terms of memory, storage, processing, and communication capabilities. This has prompted many cloud-based third-party service companies to offer external solutions like Amazon Web Services (AWS) IoT and Azure IoT. These services provide a spectrum of capabilities, including data storage, data processing, and application hosting, which can help IoT devices collect, analyze, and act on data more effectively [3]. However, entrusting sensitive data and device functionality to external providers introduces a new set of security challenges apart from already existing challenges in IoT that demand immediate attention.

In Figure 1, we illustrate the comparison between traditional and cloud-based IoT systems, denoted by a dashed line. Essential components include IoT devices like temperature sensors and smart air conditioners, a local server in traditional IoT setups, an IoT gateway, and the cloud in cloud-based systems, all interconnected to end users through mobile apps. The IoT system is a complex ecosystem of interconnected components that collect, process, store, and control data from IoT devices. This interaction is fundamental to the seamless functioning of the entire system. However, the involvement of third-party systems introduces a new dimension to this ecosystem, one that requires careful consideration, particularly in terms of security. For example, inadequately secure third-party systems may lead to data leaks, compromising the integrity of the IoT ecosystem. Moreover, the diversity of IoT components introduces additional security challenges, as each component may possess unique vulnerabilities. Consequently, prioritizing robust security measures becomes imperative for ensuring the resilience of IoT systems, especially since these devices frequently interact with human users and are sometimes connected to critical infrastructure.
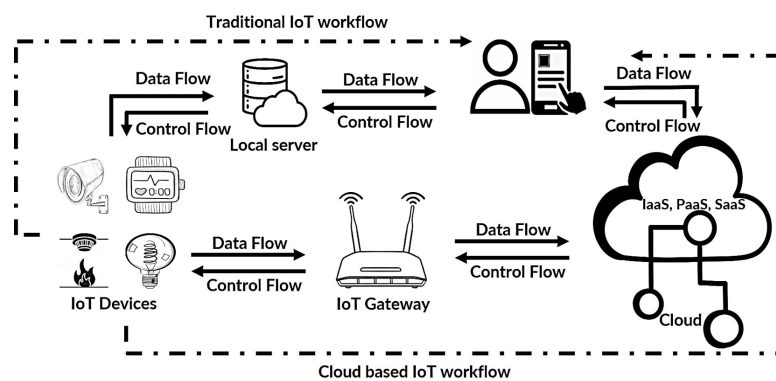

Figure 1. IoT cloud ecosystem model.

Cloud-based IoT has transformed our lives, making homes smarter and more convenient. However, as it expands into critical areas like consumer devices and transportation, addressing security vulnerabilities becomes crucial. Despite efforts by major cloud providers like AWS, Microsoft Azure, Google Cloud, and IBM Cloud, security remains a significant concern. This has drawn substantial attention, prompting researchers to actively identify vulnerabilities in the existing IoT infrastructure [4–10].

For example, a hacker could exploit a vulnerability in a wearable device to access users' personal health data. Jin et al. [11] discovered vulnerabilities in 36 cloud-based IoT devices, including the 'Hippokura' medical IoT system, where an attacker could gain unauthorized access and read conversations between patients and doctors. Additionally, incidents where an attacker hacks into a smart car's system to take control of the vehicle could become common in the future. To make matters worse, an attacker can lure a vehicle to a different location than intended using a 'GPS deception attack' [12].

The integration of IoT with cloud systems involves continuous communication, making them susceptible to adversarial attacks, eavesdropping, MITM attacks, and packet tampering [13,14]. These security concerns are critical, especially for IoT devices in essential systems like power grids, where a cyber attack could cause widespread outages. Multiple IoT systems relying on cloud infrastructure pose significant security risks.

The rapid development of IoT systems often prioritizes cost over security, creating exploitable vulnerabilities. Manufacturers frequently neglect device security, viewing the cloud merely as a platform. IoT's distributed architecture and communication complexities pose unique security challenges [11]. Despite ongoing research, there are a lack of frameworks to systematically categorize IoT devices for addressing security issues, hindering the development of effective security measures.

We aim to review security issues in cloud-based IoT systems and address gaps in the literature, motivated by the need for a targeted security approach. Unlike existing studies [15,16] that focus on isolated IoT scenarios, this paper categorizes cloud-based IoT into ten distinct types, each with unique challenges, and proposes tailored mitigation strategies. We highlight the importance of addressing these issues amid evolving technologies and regulatory demands. This leads to the following research questions:

- RQ1: can we comprehensively categorize the various cloud-based IoT devices based on their specific purpose and address their existing or future security/privacy issues?
- RQ2: what mitigation approaches can be employed in each category to address the identified security/privacy issues?
- RQ3: how can standardized verification protocols be customized to balance security and usability across all distinct IoT categories?

In our article, Figure 2 outlines the key sections, providing an overview of the structure, while Figure 3 provides an overview of the main content, emphasizing key challenges and corresponding mitigation strategies. We begin with a system model to understand security challenges, followed by blocks that examine security/privacy risks and mitigation approaches. The final block showcases real use cases addressing these issues.

The rest of this article is structured as follows: Section 2 covers the IoT cloud ecosystem model, literature review (Table 1), and our novel contributions. Section 3 categorizes IoT challenges and solutions, addressing RQ1 and RQ2. In Section 4, we explore the way forward (RQ3), culminating in our conclusions. We have included a summary table (Table 2) at the end that consolidates the key points from each category for quick reference.
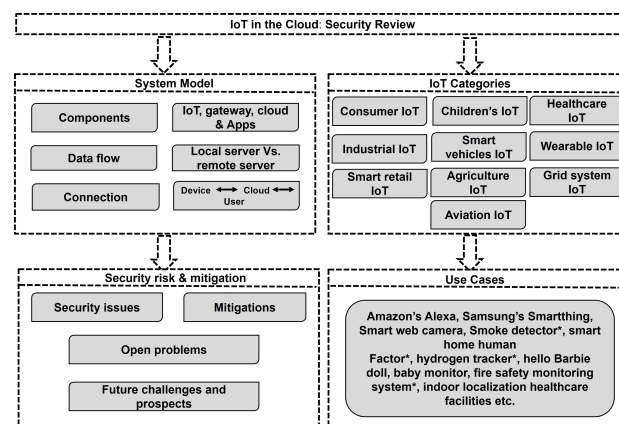
Figure 2. Article framework. This figure outlines the system model, IoT categories, security risks, mitigations, and related use cases. The 'Use Cases' represent real-world scenarios that illustrate the identified security issues or demonstrate the application of proposed mitigation strategies. While some use cases highlight cloud-based IoT systems, others showcase IoT systems transitioning toward cloud integration, emphasizing the relevance of the cloud in their future evolution.

Figure 3. Overview of the article, highlighting key security challenges and providing examples of mitigation strategies.

2. Background and Related Work

This section delves into the fundamental concepts of IoT and cloud computing. We explore how these separate domains mutually benefit. However, it is noteworthy to acknowledge that this integration also brings forth concerns regarding security and privacy [17].

2.1. IoT Cloud Ecosystem Model

Traditional IoT relies on localized data processing, offering better control but limited scalability. In contrast, cloud-based IoT enables real-time analytics and high scalability via cloud storage but introduces risks such as reliance on central storage, trust issues, and amplified privacy concerns. While data breaches affect both systems, the aggregation of sensitive user data in cloud-based IoT increases the attack surface, necessitating robust trust and privacy safeguards.

IoT devices form a connected system enabling electronic devices and sensors to communicate via the internet, enhancing daily life. Modern IoT cloud systems go beyond traditional frameworks, supporting large-scale implementations that serve millions of users and manage vast amounts of data from IoT devices [18]. In this context, the IoT gateway (refer to Figure 1) connects IoT devices to the cloud, enabling local communication and edge data processing. A key feature of cloud-based IoT systems is interoperability through standard protocols like HTTP PUT and GET requests, allowing user access. The IoT hub is another essential component, enabling various devices, manufacturers, and users to join the IoT ecosystem [19].

2.1.1. IoT Systems

The concept of IoT revolves around the idea of "smartness", enabling devices and sensors to autonomously acquire and apply knowledge [20]. An IoT system is a network of interconnected devices, sensors, and software that collect, exchange, and analyze data, each presenting unique security challenges.

2.1.2. Cloud Computing in IoT

Cloud computing's three service models—Infrastructure as a Service (IaaS, e.g., Amazon Web Services), Platform as a Service (PaaS, e.g., Microsoft Azure), and Software as a Service (SaaS, e.g., Google Apps)—benefit IoT devices based on their specific needs [21]. It offers massive data storage, scalability, computational power, and infrastructure to support the extensive data processing and analytics required for IoT applications [22].

2.2. Literature Review and Surveys on IoT Security and Privacy

Research often lags behind, leaving gaps in addressing security challenges at the intersection of IoT and cloud computing. For instance, Thakor et al. [23] highlight the challenge of securing resource-constrained devices and proposing cryptographic solutions. As IoT systems increasingly rely on cloud computing, recognizing the importance of cloud integrations and their associated security risks is urgent, as shown in Table 1. However, these studies often lack systematic categorization of IoT vulnerabilities across scenarios like healthcare, children's IoT, and agriculture, while offering limited insights into open challenges and future directions in cloud-integrated IoT.

In this direction, Chen et al. [24] highlighted rising security risks with the increased use of IoT devices and cloud computing in consumer applications. They identified vulnerabilities like weak passwords, unsecured communications, and poor access controls. They recommend implementing strong security measures and educating consumers about risks and protections.

Table 1. Comparison with recent surveys.

Publication (Year)	IoT Challenges	Cloud Challenges	Mitigations	Use Cases
[25] (2017)	◑	○	◑	◑
[3] (2017)	○	○	○	◑
[1] (2019)	●	○	◑	○
[26] (2019)	●	○	◑	●
[20] (2020)	◑	○	○	◑
[27] (2020)	●	○	●	◑
[28] (2020)	○	●	◑	◑
[29] (2021)	●	◑	●	◑
[23] (2021)	●	○	◑	◑
[24] (2021)	◑	●	◑	●
[30] (2022)	◑	○	○	○
[31] (2022)	◑	○	○	◑
[15] (2023)	●	○	●	○
Our survey (2024)	●	●	●	●

Full cover: ●, partial cover: ◑, not covered: ○

Almolhis et al. [28] highlighted new security concerns when smart homeowners' data are stored and processed in third-party clouds. While these studies focus on specific domains like smart homes, they lack a unified framework for vulnerabilities or strategies for areas like children's and healthcare IoT. Our work fills this gap by systematically categorizing IoT into ten types and addressing their unique challenges. Studies on smart cities, logistics, buildings, homes, and retailing reveal inherent IoT security issues like

interoperability, privacy, and scalability [32]. Sivaraman et al. [33] emphasized the security challenges related to IoT systems. Similarly, Harbi et al. [26] studied the various taxonomy of security requirements related to IoT along with their mitigation approaches. Digital forensics is also impacted by IoT security concerns [34]. While promising solutions exist [35], IoT-cloud integration is still emerging, bringing additional complexities and unaddressed security challenges as more private players enter this field.

Modern IoT cloud systems consist of large-scale systems and cloud applications with millions of users, generating vast amounts of data. Protecting these devices and the data presents a significant challenge, especially in the absence of uniform laws and regulations for deployment and development [11]. The marriage of IoT and cloud technology has sparked a revolution in the production of IoT devices and increased security vulnerabilities. The vast amount of data collected by these devices, often personal and sensitive, makes them prime targets for cyber attacks. This study builds on previous work by proposing a comprehensive framework that categorizes cloud-based IoT systems into ten distinct types, addressing both systemic vulnerabilities and specific domain-related security issues. Unlike the prior literature, we focus on underexplored IoT domains and highlight actionable insights for mitigating risks. Given the growing complexity of these threats, a systematic approach becomes crucial. Categorizing vulnerabilities based on their nature enables the development of targeted defense mechanisms. Through this categorization, we can design more effective security solutions to mitigate these risks and ensure the safety of these devices.

2.3. Uniqueness of Our Survey

This article introduces a comprehensive classification system for IoT security vulnerabilities, categorizing them into ten distinct groups based on the purpose and application of IoT devices.

Why Ten Categories of Cloud-Based IoT?

The rationale behind selecting ten categories lies in their ability to comprehensively encompass the diversity of use cases and their unique security challenges. We derived these categories based on an extensive review of the existing literature, current IoT applications, and the security vulnerabilities. In our study, each category showcases a significant domain where cloud-based IoT introduces unique challenges which necessitate targeted mitigation strategies.

We consider the following criteria for selecting these specific categories:

- Relevance to Major IoT Domains: each category is tied to major IoT domains, such as consumer IoT, healthcare IoT, or agriculture IoT, which are widely adopted and significant in real-world applications.
- Distinct Security Challenges: the categories were chosen to address scenarios posing specific vulnerabilities, such as centralized data breaches, malicious access, or system disruptions.
- Diversity of Use Cases: the ten categories collectively cover a broad spectrum of IoT use cases, ranging from critical infrastructure and healthcare to consumer devices and smart environments.
- Scalability and Adaptability: our category classification ensures that as IoT use cases evolve, our framework remains flexible enough to accommodate emerging domains or new categories.

For example, consumer IoT, such as voice assistants, faces unique threats like voice squatting attacks, where malicious user can exploit ambiguities in voice commands to gain unauthorized access. Similarly, healthcare IoT devices, including medical devices, are highly vulnerable to private data breaches that compromise sensitive patient information,

posing significant risks to both privacy and safety. Meanwhile, industrial IoT, which powers life critical infrastructure, is particularly susceptible to attacks targeting operational integrity. This systematic approach ensures that the classification captures the most prevalent and significant IoT domains while providing a strong framework for addressing both existing vulnerabilities and emerging threats as the IoT landscape continues to evolve.

To address our research, we defined three key questions. The first question (RQ1) involves categorizing IoT devices into ten distinct groups by purpose and function, as shown in Figure 2, to identify their specific security and privacy issues. The second question (RQ2) explores various mitigation strategies for these issues and identifies remaining challenges that need further study. Finally, the third question (RQ3) assesses the feasibility and effectiveness of a standardized security solution across all categories, with a focus on finding the next best solution if a uniform approach is unworkable.

3. Categorical Study on Cloud-Based IoT, Their Security and Privacy Challenges, Mitigation Approach, and Open Problems

This section elaborates on the security challenges associated with each of the ten categories (RQ1) and their corresponding mitigation approaches (RQ2). Additionally, we have dedicated a section to open problems that highlight security issues requiring future attention and resolution. Consequently, the following section provides responses to both RQ1 and RQ2.

3.1. Category 1: Consumer-Oriented IoT

3.1.1. Security Challenges

Consumer-oriented IoT devices, like voice assistants, enhance convenience but pose significant security and privacy risks. A major issue is the **voice squatting attack (VSA)**, where devices dependent on third-party natural language processing can be compromised. Cloud servers like Amazon and Google do not guarantee security against vulnerabilities, allowing malicious third-party apps to access and potentially steal sensitive user data.

Precise accuracy in voice command recognition is crucial for reliable performance in voice-based systems. Attackers may use voice synthesis or replay attacks to mimic users, potentially accessing financial accounts [36]. Attackers may also install malicious apps on users' phones, increasing the risk of financial loss [37–39]. Notable speech-based IoT devices such as Google Assistant, Apple's Siri, and Microsoft's Cortana are widely used, highlighting the urgent need to enhance security to protect user privacy and prevent attacks.

Interoperability issues and **unauthorized access** are key security concerns for cloud-based IoT. Interoperability problems arise when devices allow multiple apps to coexist, such as Samsung SmartThings, which is vulnerable to 20 different security threats [40]. Samsung SmartThings is an IoT device that uses Linux OS and supports ZigBee, Z-wave, and Bluetooth. Its frequent data transmissions make it highly susceptible to cyber attacks [7,41–43]. Footnote text removed. Attackers can exploit these channels through vulnerabilities like unsecured data transfer protocols or MITM attacks, compromising user security and privacy [14]. These breaches allow unauthorized access to networks and remote manipulation of devices, threatening data privacy and synchronization. Additionally, source code flaws could give apps excessive privileges, enabling them to spy on other installed applications. Reliance on a single-factor authentication mechanism, like a password, makes users prone to brute-force attacks [44], where attackers can try a large number of passwords to gain access. Sharing the same Wi-Fi network with an attacker makes it easier for them to steal passwords and initiate unauthorized actions. Furthermore, bugs in SmartThings's code, varying programming styles, and the utilization of the "If This, Then That" (IFTTT) platform introduce vulnerabilities and potential command injection attacks [45]. Concerns

over the security of Wi-Fi networks are heightened by the vulnerabilities inherent in Smart-Things systems. Notably, the trigger-action rules in the IFTTT platform can be bypassed, conflicts can arise, and actions may be repeatedly executed, leading to denial of service attacks (DDoS) [46]. Not confined to particular devices like SmartThings, DDoS attacks are recognized as particularly vulnerable targets, notably emphasized by the 2016 Mirai botnet attack, acclaimed as the most extensive of its kind in history [47]. Ensuring robust security measures and addressing these vulnerabilities is essential to safeguard the integrity and privacy of IoT systems utilizing SmartThings and the IFTTT platform. In addition to the vulnerabilities discussed earlier, another significant security concern arising in this category involves the potential for MITM. These attacks include a shared private key to encrypt a task linked to a specific assistant, like Amazon Alexa or Google Assistant [29].

In such attacks, hackers can intercept and decrypt sensitive information exchanged between the IoT cloud and the assistant, compromising the integrity and confidentiality of the data. The IoT devices sharing the same network or relying on Wi-Fi are more susceptible to MITM attacks [48,49]. Many consumer-oriented devices are vulnerable to data leakage due to inadequate protection. This weakness raises another significant security issue due to inadequate protection, making the device vulnerable to data extraction via reverse engineering [50]. Essential elements such as certificates, keys, algorithms, private authentication, and other sensitive personal human behaviors (such as motion and voice) are often stored within this flash memory (storage device) device, making them a prime target for malicious actors [51].

Furthermore, many IoT consumer-oriented IoT devices are susceptible to unprotected debugging interface vulnerabilities, which can be exploited by attackers to gain unauthorized access and misuse [52]. Many IoT devices are often left unprotected by manufacturers despite being intended for device debugging purposes. Intruders can access device shells to manipulate or inject harmful commands, leading to device damage and security breaches. Issues like data leakage and debugging further compound security concerns, particularly in devices like smart cameras [53–56].

The persistent use of hardcoded passwords poses significant security risks in many IoT devices, such as smart cameras. These passwords, often stored in unprotected flash memory, are easily cracked and can only be changed by manufacturers, complicating updates or resets if compromised. Additionally, some cloud-based IoT devices have flawed authentication mechanisms, overly dependent on static identifiers like MAC addresses, which can be exploited to disrupt connections between the camera and the cloud server.

The security of IoT devices is often compromised by the lack of authentication in data transfer from devices like cameras to the cloud, enabling attackers to easily upload videos via constructed URLs. Insecure communication protocols, such as using unencrypted HTTP instead of HTTPS and simplistic proprietary protocols, allow attackers to intercept communications, decode video streams, and access sensitive information like app SSIDs and passwords for remote camera connectivity.

Another authentication-related security issue arises due to the use of fixed hash value, which persists in many current cloud-based IoT devices including hue light bulb [57]. The vulnerabilities in interconnected devices, which are essential components of cloud-based IoT systems, are also contributing to the growing security concerns [58–60].

Weak authentication practices in smart home devices can lead to unauthorized access and data breaches, especially when multiple devices are interconnected. These vulnerabilities could be exploited by third-party companies to collect user data for targeted advertising or selling purposes. Shared use of devices like smart speakers among family members increases the risk of unintended access and privacy breaches, particularly if user data are not deleted from cloud servers when a user stops using the device. Additionally, weak

authentication practices heighten vulnerability to unauthorized access and enable excessive data collection from users by cloud-based IoT devices.

Researchers have raised concerns over the amount of data these devices send to cloud servers, often in the form of unencrypted data packets with unknown content [61,62]. This discrepancy in data size and content raises suspicions about the devices' communication. Studies have shown that even with the restriction to send only a small amount of 20 KB of encrypted data, the server can still trigger emergency notifications on the users' app, suggesting the data likely include private information collected without the user's explicit consent. For instance, researchers found excessive data collection loopholes in Nest smoke alarms [62]. There are concerns about the device collecting potentially sensitive data beyond intended functionality, as it captures human movements and assesses user states based on lighting conditions. Addressing these security issues is crucial to ensure the privacy of users and build trust in smart home technologies. We will now present some of the available solutions in the following section.

3.1.2. Mitigation Approaches

As we acknowledge that virtual personal assistants (VPAs) are vulnerable to **voice squatting attacks (VSAs)** and **voice masquerading attacks (VMAs)**, several mitigation approaches have been proposed. One such approach developed by Zhang et al. [38] is a mitigation technique to address voice masquerading attacks in VPAs.

- The approach involves: (1) Phonetic analysis to detect similarly pronounced invocation names. (2) Natural language processing (NLP) to understand user intent and context. (3) Machine learning to identify patterns and flag suspicious activity.
- When a risk is detected, the system captures the ongoing impersonation threat and then alerts the user in real time to prevent data breaches.

This technique strengthens VPA security and protects sensitive user data. Another proposed solution includes the voice authentication technique [63]. This work advocates for the use of a voice spoofing detection framework which integrates four modules for effectively securing speaker verification in voice-based IoT devices. Hooda et al. [64] proposed a systems-oriented defense against voice-based confusion attacks where an attacker exploits ambiguities in voice commands to mislead VPAs into triggering malicious actions or skills instead of intended ones. Termed SkillFence by the author, it is a browser extension designed to thwart voice-based confusion attacks targeting voice assistants, such as Amazon Alexa. Concurrently, researchers are actively seeking optimal solutions to address interoperability challenges in IoT devices, including platforms like Samsung SmartThings. Similarly, Chatterjee et al. [65] developed a lightweight identity-based cryptosystem employing a physically unclonable function (PUF) suitable for IoT to enable secure authentication and message exchange among the devices.

Nazzal et al. [66] proposed a multi-stepped categorization of SmartThings vulnerabilities based on the platform's component and nature of the attack and thus proposed relative mitigations. Consumer-oriented IoTs are particularly vulnerable to **DDoS** attacks, which are currently one of the most serious virtual threats. Emerging technologies like **software-defined networking (SDN)** can help mitigate DDoS attacks for IoT devices. One of the mitigation approaches for DDoS attacks through SDN is **flow filtering.** The flow filtering strategy is a straightforward approach that uses centralized control to block or allow network traffic based on packet header information. While the use of software-defined networking (SDN) to mitigate DDoS attacks is promising, implementing SDN in consumer IoT devices faces scalability and cost barriers. Moreover, deploying flow filtering or rate-limiting approaches in resource-constrained devices could lead to bottlenecks and performance degradation.

However, it may cause delay and bottleneck issues due to statistics gathering and packet inspection [67–69]. The **honeypot technique** is another mitigation approach that creates a simulated environment to collect information about malicious traffic and can be used with SDN to update detection and mitigation policies [70]. Security applications usually adopt a rate-limiting approach in conjunction with deep package inspection procedures. The idea implies that to prevent network overload caused by volumetric attacks (a massive volume of traffic), SDN controllers can set a traffic volume limit and reject subsequent traffic when the limit is reached, often used in combination with Deep Package Inspection procedures for enhanced security [70].

Moving Target Defense (MTD) is another DDoS mitigation approach that involves dynamically reconfiguring a network/system based on random values to prevent attackers from making the system unavailable. This includes techniques such as randomizing IP and MAC addresses to prevent DDoS attacks. However, there are concerns about the impact on performance and cost when deploying MTD on large-scale networks [71,72]. MTD involves dynamically reconfiguring a network to prevent attackers from making it unavailable [72] while another approach, Traceback, uses the packet header information to identify an attacker's origin. SDN's control plane provides a holistic view for effective mitigation solutions [73].

In response to security concerns, researchers have proposed several solutions to strengthen the security of cloud-based IoT devices. One such approach is the secure IoT structural design for smart cities proposed by Bhattacharjya et al. [74]. This design applies to various contexts, including smart homes and the Power Internet of Things (PIoT).

- The approach leverages a three-layered security framework: (1) perception layer, (2) network layer, (3) application layer.
- The approach employs a hybrid RSA cipher, which combines public and private key encryption for secure and efficient data transmission, to ensure robust architectures in IoT devices.
- Cryptographic algorithms are foundational elements of such secure design. They provide a layer of encryption to protect data confidentiality and integrity during communication between devices and the cloud.

Cryptographic algorithms can prevent security threats to a certain extent for smart homes or smart cities [75]. However, there are certain technical issues with the application of high-end security to these IoT devices due to their low computing power, limited space, short memory, and limited battery life [76]. Thus, a lightweight encryption such as Piccolo or PICARO [23] offers a better balance between the security and resource constraints of IoT devices. The smart home IoT devices are heavily vulnerable to private and sensitive data of consumers, and, in this direction, Gerber et al. developed **LOKI**, an interface that enables control of a smart home using local information processing and protecting smart home systems from hacking attacks [77].

3.1.3. Open Problems

Security solutions using SDN could mitigate common IoT issues like DDoS attacks but face challenges due to IoT complexity and diverse attack methods. Additionally, manufacturers often neglect regular firmware updates for IoT devices, jeopardizing the future security of IoT and cloud ecosystems. Key concerns include the reliability of cloud providers, inconsistent firmware updates, absence of standards, privacy risks, and complex security strategies. Addressing these will necessitate cooperation among manufacturers, cloud services, policymakers, and consumers.

3.2. Category 2: Children's IoT (Smart Toys)

3.2.1. Security Challenges

Children's IoT devices, tailored for entertainment, development, and education, feature specialized sensors and firmware for personalized interactions with kids. These devices are subject to stringent privacy regulations like the COPPA rule [78], which mandates confidentiality and security for online services aimed at children. Inadequate data security in these devices can lead to significant privacy risks.

Insecure communication channels, weak authentications, and limited parental control over data collection and setting further intensify these concerns. For instance, a case study by Chu et al. [8] revealed that the hydrogen tracker, a children's IoT device, violates COPPA rules. Interestingly, cloud-based IoT toys are vulnerable not only to children but to everyone in the home who owns them. The statement "Someone is watching through Barbie's eyes" holds enough significance to warrant sharing it with every household member, as it highlights the vulnerability at stake [79]. These are open to eavesdropping attacks by malicious users [80].

Ling et el. [30] concluded that **data security** has emerged as a growing concern regarding children's IoT. **Jamming attacks** are one of the prominent attacks found in entertainment-based drones where the malicious user intentionally captures and manipulates drone data via unauthorized transmitting channels [16]. These drones and vibrators also carry privacy concerns, as the attacker can access sensitive information, including videos and audio stored on cloud servers, shared by children with these toys. The hydrogen tracker, a type of IoT device designed for monitoring a baby's hydrogen level, exhibits security vulnerabilities both in its cloud infrastructure and user applications [5,8,79,81,82]. The access control mechanism between children's IoT devices and cloud servers has vulnerabilities, allowing attackers to intercept authentication packets. This flaw lets attackers access sensitive information, such as profile images, and manipulate cloud services to retrieve user files. The devices communicate with servers using HTTP GET and POST requests, which has led to reported security issues, including token reuse problems in systems like the hydrogen tracker.

For instance, in the hydrogen tracker, whenever the child drinks water, the user app sends this information to the cloud. Here, the attacker can capture the packets containing the authentication token and the HTTP header information and upload fake content to the cloud. These fake data can disrupt the proper functioning of the hydrogen tracker and potentially lead to misdiagnosis or improper treatment decisions. The URL token for the user pictures contains 12 letters. On the cloud side, it returns the HTTP 301 response as long as the first three letters pair with the legitimate token. However, the cloud returns HTTP 404 for the nonexistent token. This helps to reduce the time needed to guess the correct tokens. When combined with the two security risks, the attacker can easily use brute force to exhaust the remaining 9 letters, and, hence, the user profile is leaked.

A significant security issue is the failure to delete expired files from the cloud, leading to privacy breaches when new profile images remain linked to old ones. Referring to the security issues for the children's IoT application side, researchers primarily acknowledge three main issues.

(1)   The primary concern is the presence of third-party services integrated into the user application, posing a substantial security vulnerability. In the case of the hydrogen tracker, the mobile app utilizes four third-party analytics and performance monitoring services. Although the traffic data are encrypted, it remains uncertain whether private data are being leaked through these services.

(2)   Another concern arises from the use of plain-text APIs in applications. This lack of data encryption during transmission to the cloud server heightens the risk of privacy breaches, including eavesdropping.

(3)   The attacker can obtain the intermediate packets exchanged between the app and the cloud, enabling packet spoofing. Spoof packets may change the codes and cause the app to malfunction.

The attacker can intercept packets exchanged between an app and the cloud, leading to personal data leaks. Additionally, when network errors occur, user apps send crash reports containing personal details like name, age, and weight to third-party IoT developers, inadvertently exposing sensitive information. A major security flaw in many children's IoT devices is the persistent enabling of remote access post-release, which offers attackers a straightforward way to exploit these vulnerabilities [83].

Furthermore, the use of plain-text API for communication between the IoT device and the cloud significantly increases the risk of unauthorized data interception. A prevalent security issue observed in both consumer-oriented devices and children's IoT devices involves the storage of fixed user data in the IoT memory card, which can be easily accessed by malicious individuals if the card is detached. This vulnerability raises concerns about the potential exposure of sensitive user information to unauthorized parties. Having an active default development account in the IoT device, which grants root privileges and has vulnerable passwords, presents a major security risk. This allows attackers to effortlessly access sensitive information and exploit the devices' vulnerabilities. In addition to these existing issues, children's IoT devices face other critical issues, including inadequate protection of the universal asynchronous receiver/transmitter (UART) interface. Commonly used for troubleshooting, the UART's conventional method makes it easy for attackers to manipulate device parameters and extract sensitive information [84].

In addition to the previously mentioned security issues, many children's IoT devices suffer from security flaws attributed to weak authentication and the use of plain-text API. These vulnerabilities undermine the overall security of the devices, making them more susceptible to unauthorized access and potential data breaches. It is crucial to address these weaknesses by implementing stronger authentication mechanisms and ensuring secure communication protocols to protect user data and maintain the integrity of IoT systems.

3.2.2. Mitigation Approaches

Children's IoT has the potential to collect terabytes of sensitive personal, contextual, and usage information, which may be a subject of cybercrime. In smart toys' hardware restrictions, a specific encryption and authentication mechanism is required. In this direction, Rivera et al. [85] designed and built specific security mechanisms for the smart toys and also validated them on the platform.

Children lack an understanding of privacy and online safety, especially in social media and cloud environments. Rafferty et al. [86] proposed a model that somehow puts the obligations for children's privacy on parents or guardians and alerts them in case of any violation. Similarly, Yankson et al. [87] presented an abstract forensics investigation framework focused on using non-conventional means that allow investigators to successfully "Plan", "Preserve", "Process", and "Present" (4P) as a systematic means to conduct digital forensic analysis.

3.2.3. Open Problems

Children's IoT devices pose notable security and privacy risks due to young users' lack of awareness. Many devices fail to inform parents about potential privacy breaches. Therefore, it is essential that these IoT devices include notifications or mechanisms that

require parental supervision for their operation. Any forthcoming IoT devices must comply with regulations like COPPA and similar guidelines specifically designed for children's IoT.

3.3. Category 3: Healthcare IoT and Medical Equipment

3.3.1. Security Challenges

Healthcare IoT, including wearables, implants, and remote monitoring, improves patient outcomes, reduces costs, and personalizes care. Post-COVID-19, interest in IoT devices, especially in healthcare, has surged. IoT healthcare solutions have proven to significantly enhance patient care and save millions of lives. Some of the examples are remote patient monitoring (RPM), decentralized clinical trials (DCT) [88], pulse oximeters, glucometers [89,90], etc.

The significant shifts in IoT devices in healthcare offer staggering benefits but also elevate the risk of cyber attacks on interconnected medical devices. Many cloud-based medical devices transmit unencrypted data, creating vulnerabilities. Attackers could manipulate these data, disrupting treatment plans and jeopardizing patient well-being[91]. Healthcare institutions utilize a range of IoT devices for accurate patient and asset tracking, commonly referred to as indoor localization facilities in healthcare [6,92,93]. Indoor localization facilities for healthcare face significant security vulnerabilities in both IoT and cloud server environments. Two primary concerns are prevalent. First, **weak password security** is common, with devices often using default, widely known passwords. Second, there is inadequate memory protection. Many IoT devices include built-in SSH services, compounding the risk when default passwords are not changed.

A critical security issue is the use of default passwords on devices, making them easy targets for attackers. This vulnerability can compromise entire systems and expose sensitive patient data. The second issue is insufficient memory protection. Devices in public areas can be easily removed, and sensitive data on memory cards accessed. On the cloud side, a major vulnerability exists where communication between the cloud and server uses unencrypted plain-text APIs. Healthcare facilities transmit database credentials every few seconds without proper protection, making them susceptible to interception over unsecured Wi-Fi. Attackers can exploit this to access log files or disrupt device functionality through denial-of-service attacks [6].

Moreover, cloud-based pulse oximeters and glucometers, which store health data offline, are susceptible to **hijacking attacks.** In such scenarios, unauthorized access to all offline readings becomes straightforward for hackers after obtaining user credentials [94]. Cloud-based health image IoT systems face issues with data integrity, availability, and confidentiality due to unencrypted processing of medical image data between IoT devices and the cloud. To address this issue, Jin et al. [11] analyzed access policies in 36 IoT devices, which included medical equipment. The authors discovered several design deficiencies within the access control mechanism of medical devices provided by established companies. These deficiencies, such as overly permissive settings or a lack of proper authentication, could allow several unauthorized users to access various sensitive health data, such as blood pressure, age, height, and weight, for all consumers of specific medical equipment companies, such as Biobeat and Hippokkura (used as a case study).

Many medical IoT devices are vulnerable to hardware attacks. Attackers can implant hardware trojans during chip manufacturing, compromising device functionality and integrity and posing risks to patient safety [95]. The U.S. Food and Drug Administration (FDA) has expressed serious concerns about this, issuing reports indicating instances of tampering with patients' health data that occurred after modifying the hardware of medical IoT devices [96,97].

The use of drones in healthcare has surged, especially for collecting samples, delivering medications, and supplying resources. [98]. However, this deployment of drones also brings several vulnerability issues, such as replay, MITM, impersonation, and privileged-insider attacks. These vulnerabilities stem from the wireless nature of communication between deployed drones and their ground station servers. For instance, in **replay attacks**, the attacker intercepts the communication between the drone and the ground station and later replies to that communication to deceive one of the parties. Similarly, in an MITM attack, a malicious user secretly intercepts and possibly alters the communication between two parties without their prior knowledge. Meanwhile, privileged-insider attacks involve a legitimate person with authorized access to an organization's resources and information misusing that information access for malicious purposes. These medical devices not only enable attackers to compromise security systems but also expose patients' health data to the risk of being accessible to the public.

3.3.2. Mitigation Approaches

Various techniques can help mitigate security issues in medical IoT. One such approach focusing on location privacy was proposed by Alishahi's group [99].

- This technique utilizes multiple anonymization methods, including k-anonymity, ℓ-diversity, t-closeness, α-anonymity, and δ-presence, to offer online location-based healthcare services while ensuring robust protection of patient location data.
- However, there is a trade-off that this technique might produce some data obfuscation, impacting the accuracy of exact location tracking in some cases.
- This prioritizes user privacy but might limit the precision of location-based services. To safeguard against unauthorized access and data breaches in drone-aided medical services, it is crucial to implement reliable authentication, access control, and key management schemes in the IoT environment.
- These preventive measures ensure that only authorized users can access sensitive data transmitted by drones, protecting patient privacy and sensitive information.

Additionally, incorporating Blockchain mechanisms with authentication deployment can further enhance its robustness against various types of attacks. Blockchain technology can assist in ensuring a transparent audit by maintaining a secure ledger [100], making it difficult for attackers to manipulate or steal sensitive medical information. To mitigate such issues, Bu et al. [101] proposed a robust approach, Bulwark, for guarding against existing and potential communication-based attacks on implantable medical devices. This secure protocol allows authorized third-party medical teams to securely access the internal memory device (IMD) in emergencies. Bulwark can address not only MITM but potentially other communication vulnerabilities as well.

Ma et al. [102] proposed the use of **Time Modulated Arrays (TMAs)** to improve covert communication in IoT systems, offering a low-complexity alternative with enhanced beamforming precision and timeliness, which could be particularly valuable for drone-assisted IoT applications. Wazid et al. [98] proposed another approach that leverages a **private-Blockchain-based technology** to establish secure communication in an IoT-enabled drone-aided healthcare environment.

- This framework utilizes a secure voting mechanism to ensure the authenticity and integrity of data transmission.
- This mechanism involves mining, verifying, and adding blocks containing medical requirements in the P2P network, all based on the PBFT consensus algorithm.
- The security analysis performed on the proposed framework demonstrates its ability to withstand various potential attacks. Furthermore, the framework has been practically implemented through a Blockchain simulation.

ML-based approaches are also one of the potential solutions for detecting attacks on healthcare systems. ML can analyze vast datasets of network and device behavior to identify patterns that deviate from normal functioning, potentially indicating malicious activity. In this direction, Saeedi et al. [103] demonstrated how a decision tree algorithm can be used to detect malicious attacks on healthcare IoT devices.

HealthGuard is a novel machine-learning-based security framework that observes the crucial signs of different connected devices of a medical IoT and correlates the crucial signs to understanding the changes in body functions of the patient to distinguish benign and malicious activities. The authors have used four different (artificial neural network, decision tree, random forest, k-nearest neighbor) ML-based detection techniques [104].

Techniques such as Blockchain and machine learning for healthcare IoT systems offer robust solutions; however, they require high computational power and substantial storage, which are not feasible for resource-constrained medical devices.

Beyond securing data transmission, robust security solutions are also essential to safeguard medical IoT devices from hardware-level attacks. Srivastava et al. [105] presented an improved method for secure data transmission between a network and storage using lightweight cryptographic techniques, such as the **ARX encryption scheme.** The ring signatures have also been introduced to the communication process, which offers significant privacy benefits, including Signer's Anonymity and Signature Correctness. In addition, the same group of researchers developed GHOSTDAG, a new Blockchain protocol that uses a directed acyclic graph to monitor the health data of patients remotely. This protocol employs smart contract programs from Blockchain technology to facilitate the monitoring process [106].

Security solutions for hardware attacks are specially designed to safeguard medical IoT from hardware-level attacks such as physical tampering [107]. For instance, Wu and colleagues introduced a "golden die" mechanism designed to identify hardware trojans with a substantial footprint, making them easily distinguishable from the standard base configuration [108]. Finally, it is worth mentioning that deep learning-based approaches have also been implemented to enhance the security and resilience of medical IoT devices [109]. Edge computing, serving as an alternative to cloud-based systems for processing data nearby, emerges as a promising solution for addressing the challenges posed by critical IoT devices. Li et al. [110] proposed solutions incorporating SDN edge computing, where edge servers authenticate medical devices before allowing them to transmit data. This approach keeps sensitive patient data localized at edge servers, minimizing the risk associated with long-distance data transfer.

3.3.3. Open Problems

Cloud-based medical IoT devices face significant security challenges, including inadequate access policies and unsecured data transmission that allow malicious interception of sensitive medical information. While AI and Blockchain offer potential solutions, they require substantial resources and computational power, complicating their implementation. Figuring out how to efficiently use these approaches remains an ongoing challenge for researchers.

Moreover, the transmission of data between the cloud and IoT devices occurs in plaintext, exposing patient data to unauthorized access and posing risks to data confidentiality, medical operations, and patient safety.

Addressing these concerns requires continued research efforts in areas such as robust access control mechanisms for cloud-based medical IoT services, secure communication protocols for encrypted data transmission, and privacy-preserving data analysis techniques.

3.4. Category 4: Industrial IoT

3.4.1. Security Challenges

Beyond the healthcare sector, security challenges are also prevalent in cloud-based industrial IoT (IIoT). Industry 4.0, marked by advanced smart technologies, has transformed industrial processes but increased attack surfaces. Examples include temperature and pressure sensors. The integration of massive data from assets and sensors into cloud servers heightens future risks [111].

Smart meters, a key IIoT technology for monitoring power consumption, face significant security challenges [112–115]. Researchers highlight two main issues: inadequate internal hardware data protection, leading to incorrect identity information and potential energy theft [115], and unprotected hardware interfaces, allowing attackers to access and modify memory by reactivating the debug interface. These vulnerabilities result in economic losses and compromised data integrity.

IIoT systems face security challenges beyond vulnerabilities in industrial devices. One major concern lies in the widespread susceptibility to DDoS attack [15,116]. In this attack, devices are overwhelmed with a flood of traffic, making them unavailable to legitimate users. In the IIoT context, this can have disastrous consequences. For instance, a DDoS attack on a power plant control system could disrupt critical operations, causing blackouts and potentially damaging sophisticated instruments [117]. Compounding these issues are vulnerabilities within the analog components of some major IIoT devices. For example, a temperature-based control system relies on an analog sensor to sense temperature. Researchers have also identified security issues related to remote tempering through electromagnetic interference [118]. The non-linear nature of sensors in these devices allows attackers to alter the output reading, potentially disrupting critical industrial processes or causing severe safety hazards. This vulnerability is not confined to temperature sensors, similar security risks have been identified in various other IIoTs such as medical, laboratory, and PID control applications [118].

Beyond vulnerabilities in industrial control systems and IIoT devices, severe security concerns are prevalent in cloud-based video surveillance systems, extensively utilized in both industrial and private settings as a means of crime prevention. In a study by Obermaier et al. [53], they examined four video surveillance systems and identified multiple security concerns, including the utilization of insecure fallback functions, weak passwords, insecure authentication processes, and the absence of robust security standards. There are also critical issues in video frame recognition, which has an accuracy of less than 90% in modern cloud-based IoT devices, particularly stemming from the use of limited eigenfaces for the principal component analysis (PCA). To improve this, a recent study using a hybrid face detection system integrated with cloud-IoT and distributed computing exhibited better face recognition with accuracy above 90% [119].

Finally, the Internet of Battle Things (IoBT), a novel iteration of IoT envisioned as the battlegrounds of tomorrow, comprises interconnected multi-devices capable of communication, action, and collaboration to achieve military objectives [120]. The reason for incorporating this IoT into industrial IoT lies in the sourcing of its interconnected devices from manufacturing sectors. These devices also possess a vulnerability in terms of security, wherein the multitude of entry points provide avenues for attackers to infiltrate any connected device across the network.

3.4.2. Mitigation Approaches

The implementation of robust hardware data protection in smart meters is presently a critical necessity for crafting resilient IIoT. To address this need, in this direction, Maritsch's group [121] proposed a hardware-secured and transparent multi-stakeholder data exchange

framework for Industrial IoT systems. This framework is designed to enable secure and streamlined data sharing among various stakeholders, including manufacturers, operators, and regulators, all the while maintaining the confidentiality and integrity of the data.

To accomplish this, the authors propose the use of hardware-based security modules, such as **Trusted Platform Modules (TPMs)**, as critical components to secure the data exchange process from the local server to the remote server. TPMs can be incorporated into IIoT devices to offer a secure means of storing and processing sensitive data, including device identities, keys, and certificates. However, a holistic approach may also involve additional measures, which include encryption protocols and secure communication channels to further strengthen the data protection framework [122]. Beyond hardware-based security solutions, other approaches have been proposed to address security challenges in IIoT systems. Tan et al. [123] proposed a Blockchain-based **Shamir's Threshold Cryptography (STC)** scheme for data protection in IIoT systems. The scheme is designed to provide secure and efficient data sharing among multiple IIoT devices while preserving data privacy and confidentiality.

- The STC scheme consists of multiple IIoT devices, a trusted authority that manages the STC keys, and a Blockchain network The IIoT devices use Shamir's secret sharing scheme to split their data into shares, which are then encrypted using the STC scheme and stored on the Blockchain network.
- The trusted authority manages the keys and controls access to the data shares.

DDoS attack pose another major threat to industrial IoT. Fortunately, researchers have proposed various novel approaches to detect and mitigate DDoS attacks in IIoT [124,125]. Performance indicators using security virtual network functions on network function virtualization (NFV) have been recently used to mitigate DDoS attacks in IIoT [124]. In this approach, various data sets were used with ML classifications to achieve very high accuracy (>99 %) in mitigating DDoS attacks in IIoTs. The results indicate that ML models implementing tree-based structures and **XGBoost decision-making trees** are the most suitable for achieving higher accuracies. This model brings out that it is not the different sizes of the networks that influence that ML, it is the fog servers.

'FLEAM' is another approach to mitigate DDoS attacks by federated learning [126]. FLEAM consists of a set of edge devices, a coordinator device, and a cloud server. The edge devices collect data and use machine-learning algorithms to detect anomalous traffic patterns, which further indicate a DDoS attack. The coordinator device aggregates the data from the edge devices and trains a global machine-learning model using federated learning techniques. Finally, the cloud server deploys the trained model to the edge devices, enabling them to detect and respond to DDoS attacks in real time. Evesti's group [127] believes that different IoT, either smart home or smart industry, can be secured via trusted network edge devices. A **rectification attack** is a type of cyber attack in which the attacker can manipulate critical temperature-based control systems. To tackle this issue, Tu et al. [118] proposed a prototype design of a low-cost anomaly detector for critical applications to ensure the integrity of temperature sensor signals. Stocchero et al. [128] suggested a secure command and control (C2) approach for IoBT by integrating the application and network layers through the utilization of an SDN-based cybersecurity mechanism.

3.4.3. Open Problems

As the IIoT continues to evolve, emerging security and vulnerability concerns accompany the introduction of new devices. In this multifaceted IIoT environment involving multiple stakeholders, the establishment of transparent data ownership, robust access control policies, and effective data governance practices becomes imperative. Without these measures, there is a high chance that sensitive data might be compromised, leading

to privacy violations. Furthermore, the efficient handling and analysis of the vast volume of data generated by IoT devices remain persistent challenges alongside well-known issues like interoperability. These challenges restrict the wider and long-term sustainability of IIoT deployments.

3.5. Category 5: Smart Vehicles' IoT

3.5.1. Security Challenges

The integration of IoT devices with advanced driver assistance systems (ADAS) in modern vehicles enhances driving comfort but introduces significant security challenges too [31]. Connected vehicles use vehicle-to-vehicle (V2V) and vehicle-to-internet (V2I) communication, improving driving experiences through critical information exchange. However, this interconnection raises concerns about sensitive data leakage and privacy risks.

Integrating IoT with the cloud increases cyber attack vulnerabilities, especially in life-critical systems. Hackers can steal vehicle data, take control of vehicles, infiltrate secure sensors, affect critical functions like airbags and door locks, and even disable the vehicle entirely.

Not limited to this, by pilfering data and deploying malicious software updates, hackers can transmit false information to drivers, initiate DDoS attacks, reprogram ECUs with infected software, and download inaccurate navigation maps.

These attacks are categorized as follows: **data authenticity attacks,** which prevent unauthorized data alterations during cloud transmission, and availability attacks, including denial of service and channel interference, exploiting bandwidth and power constraints to disrupt the IoV system's functioning [129].

- Authentication attacks on IoT vehicles (IoV) include Sybil attacks, GPS deception, masquerading, wormhole, and replay attacks.
- In Sybil attacks, attackers create fake identities to disrupt authentication and manipulate data [130].
- GPS deception leads to inaccurate location data and potential property damage.
- Masquerading involves impersonating vehicle features to infiltrate the network.
- Wormhole attacks hide the true path length between malicious nodes, causing routing errors and congestion.
- Replay attacks repetitively replay and delete messages, reducing efficiency and increasing bandwidth costs.

Data injection attack in cloud-based vehicle IoT systems pose serious risks, including loss of control, accidents, and fatalities. These attacks occur when unauthorized access exploits outdated software, known security flaws, or insufficient cloud security. Attackers can inject or alter data, causing malfunctions or unexpected behaviors. For example, false sensor data can lead to misinterpretation and accidents, while altered software may cause sudden acceleration or braking. Addressing these vulnerabilities is crucial to fully harness the potential of IoT devices [131].

3.5.2. Mitigation Approaches

The ever-evolving landscape of security threats in the connected car market necessitates continuous research and development of robust solutions. Researchers are actively exploring various avenues to combat cyber threats in next-generation autonomous vehicles [132].

Some of these studies focus on the potential risks associated with car hacking, while others delve into encryption methods, in-vehicle network communication modules, and security enhancements for Electronic Control Units (ECUs). ISAC with Massive MIMO transforms smart vehicles by enabling high-resolution sensing and reliable communication.

Zhang et al. [133] introduced a unified tensor-based framework that efficiently estimates channel and target parameters, addressing challenges such as Doppler shifts and beam squint effects. This approach enhances sensing accuracy and communication reliability, critical for applications like autonomous driving and intelligent transportation systems.

Khan et al. [134] proposed a mitigation approach like **secure software development practices**, which includes the adoption of writing secure codes, reviewing, threat modeling, and vulnerability testing. **Secure boot processes** and **hardware-based encryption methods** can secure the hardware of automotive cars. Smart vehicles must use network security protocols to prevent unauthorized access to the car's communication system. Researchers are delving into the potential of machine learning and artificial intelligence to improve the security of smart vehicles. Zewdie and Co. [135] suggested that incorporating AI/ML technology into IoT security can help combat emerging cyber threats. The paper proposes several ML/AI approaches, such as predictive analysis, threat detection and response, behavior analysis, and risk assessment, which can be used to enhance IoT security. The authors conclude that AI/ML algorithms can enhance the security of IoT devices and the cloud computing environment in which they operate by analyzing large amounts of data and detecting anomalies in real time.

In addition to AI/ML, other promising technologies are also emerging to enhance security. Blockchain-based architecture can be another solution to enhance smart vehicle security. Smys and Wang [136] argued that as vehicles become increasingly connected and autonomous, they become more vulnerable to cyber attacks. Therefore, they suggest that a **distributed ledger technology** like Blockchain can provide a secure and tamper-proof platform for managing data in smart vehicles.

- The proposed architecture consists of several components, including a Blockchain network, a smart contract layer, and a data management layer.
- The Blockchain network provides a decentralized and secure platform for storing and sharing data, while the smart contract layer enables the automated execution of contracts between different entities in the system.
- The data management layer is responsible for managing data storage and access.
- By leveraging the Blockchain's immutability and transparency, unauthorized data modification becomes easily detectable, enhancing security.

Zhao et. al. [137] addressed the problem of **false data injection attacks** in connected and automated vehicles, which can compromise the safety and performance of the vehicle. The authors proposed a **cloud-based sandboxing approach** to detect and mitigate these attacks. The proposed approach consists of three main components: a data acquisition module, a cloud-based sandbox, and a detection module. The data acquisition module collects data from the sensors and other components of the vehicle, which are then sent to the cloud-based sandbox for analysis. The sandbox simulates the behavior of the vehicle and analyzes the incoming data for anomalies that may indicate a false data injection attack. The detection module then generates an alert if an attack is detected.

3.5.3. Open Problems

While Vehicle IoT (VIoT) and its corresponding security solutions are still evolving, there remain numerous unanswered questions within this domain that demand significant attention, especially since they may pertain to critical life-related issues. For instance, ensuring the integrity of the data transmitted between vehicles and the cloud remains a challenge. Additionally, the rise of sophisticated cyber attacks targeting VIoT systems raises serious concerns about unauthorized access and vehicle control. These issues, along with the other growing risks of personal data breaches, necessitate continued research efforts to develop robust security solutions for cloud-based VIoT.

3.6. Category 6: Wearable IoT

3.6.1. Security Challenges

Wearable devices like smartwatches, medical patches, fashion items, gaming gadgets, and VR headsets are key IoT technologies, often worn close to the body and collecting various personal data. The basic architecture of a cloud-based wearable medical IoT system involves a patient wearing a health tracker (like an ECG monitor) that transmits data wirelessly to a cloud service (see Figure 4). The cloud stores and manages the patient's health information, enabling remote monitoring.
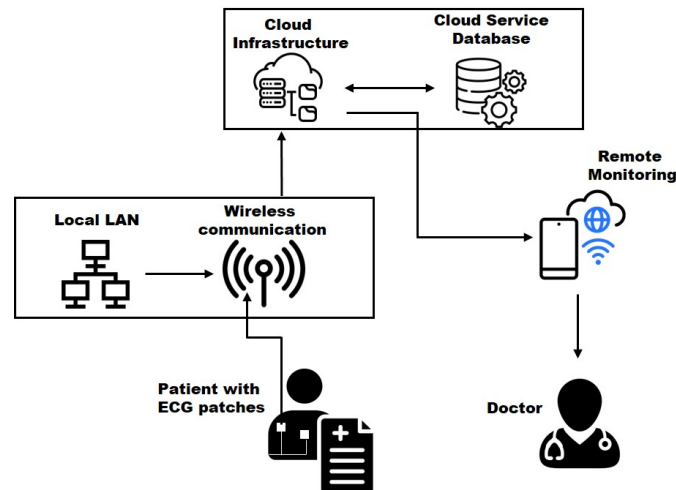
Figure 4. Basic architecture for cloud-based wearable IoT device.

While wearable IoT devices may sometimes be classified as consumer IoT, their unique characteristics—such as continuous data collection tied to personal physiological attributes and their proximity to the human body—introduce distinct security challenges. These include the risk of identity theft from lost or stolen devices, unauthorized access to biometric data, and resource constraints that limit robust security measures. These challenges differ significantly from those faced by general consumer IoT devices, such as interoperability and multi-user access issues.

Unlike traditional computing systems, WIoT devices consist of a wide range of software, hardware, and communication protocols. This diversity makes it challenging to establish a one-size-fits-all security solution, thereby impacting the ability to ensure confidentiality, availability, and integrity, collectively called the **CIA triad** [138] of the data and system functions. The diverse functionalities of WIoT devices and their intricate data lifecycle—collection, processing, storage, and transfer—expose consumers to significant security and privacy risks [139]. Worn on the body, these devices continuously collect environmental data, making them accessible to attackers. The security and privacy issues of WIoT include three factors. The first one is device architecture, the second is network connectivity, and the third is data collected by wearable devices [140]. The security concerns surrounding device architecture encompass both hardware and software aspects. Due to low-resource device features (in terms of power source, memory size, and low-bandwidth communication), it may result in severe security flaws [141]. From the software perspective, the basic operating system used in wearable devices is highly exposed to vulnerabilities [142]. Software security vulnerabilities also stem from the limited experience of programmers creating software for wearable IoT devices. Serious bugs in the software or applications are rarely identified, and the involvement of multiple parties in the development and deployment of WIoT means that no one is willing to take responsibility for these flaws.

Many IoT devices automate their functionalities, e.g., Google Glass devices. This often exposes wearable devices to security risks. Since cloud-based WIoT devices are

connected to the internet, they are highly exposed to traditional attacks, such as DDoS attacks, data leakage, MITM attacks, phishing attacks that lure users into revealing sensitive information, eavesdropping, side-channel attacks, and compromised attacks. In addition, many WIoT devices rely on weak authentication protocols, making them susceptible to unauthorized access and data manipulation during data transfer. The major concern related to wearable devices is data collection, storage, and processing. Most of the wearable IoT data include personal data that may contain sensitive information about users' habits and even financial information. Situations can become grave, specifically in the case of medical IoT, which includes a medical history, particularly heart rate, blood sugar level, and even doctor–patient conversations.

Jin et al. [11] conducted a study focusing on the security vulnerabilities of medical IoT devices, particularly those utilizing Govee technology and Amazon cloud services. Their findings revealed that simple modifications to the devices' access policies significantly compromised the confidentiality of doctor–patient communications. This vulnerability was not isolated to Govee devices alone; the authors identified similar security and privacy issues in a range of medical equipment, underscoring their susceptibility to cyber attacks. This highlights the widespread nature of security risks in WIoT devices, especially those handling sensitive medical data. Beyond the security and privacy vulnerabilities discussed earlier, the potential for theft or loss of these WIoT devices is another serious concern.

Since these devices contain personally identifiable information (PII), losing one could expose sensitive data to attackers, who could exploit them for identity theft. In the contemporary era, as the market for VR headset usage expands, privacy concerns are also escalating at a similar rate [143]. In this direction, Adams et al. [144] conducted an interview with 20 participants and concluded that to what extent the users and developers are concerned about the data collection practices in VR headsets. According to the HP security report [145], smartwatches face multiple security vulnerabilities such as inadequate user authentication, absence of encryption, and insecure interfaces. Given their widespread use in the WIoT, addressing these issues should be a top priority.

In short, some of the common security vulnerability problems with wearable IoT devices include **hardcoded password issues, code injection issues, unsecured API issues, web application vulnerability issues, and lack of proper encryption** in communication [138] and most importantly, privacy violation issues.

3.6.2. Mitigation Approaches

Well, there is no doubt that it is a complex setting and nightmare as far as securities in WIoT are concerned. Building security into solutions and platforms at every component level is crucial. As discussed earlier, weak user authentication methods expose sensitive user data to potential attackers through passive or active attacks. Fortunately, researchers are actively working to develop solutions to address these security concerns. One such promising approach is **out-of-band biometrics authentication (OOB-BA)**, proposed by Singh et al. [146].

- This method utilizes enhanced out-of-band (e-OOBA) two-factor biometric authentication to create trust relationships between users and services and protect users' data.
- OOB-BA can provide better security and minimize information leakage, and it can be an alternative authentication model for future wearable technology adoption.

Wearable IoT devices, including medical wearables like electronic skin patches, ECG, monitors, watches, fit bits, etc., are vulnerable to cyber attacks.

Kavianpour et al. [147] propose an **"Attack-Surface-Reduction by Design"** approach to mitigate security risks in medical WIoT. This framework consists of a pronged strategy.

(1) Network Traffic Analysis: The ML technique is used to analyze network traffic patterns of IoMT devices to identify anomalies that may indicate a potential cyber attack.

(2) Attack Surface Reduction by Design: The authors propose a set of guidelines for reducing the attack surface of IoMT devices. This includes hardening the devices' firmware and software, limiting their functionality to only what is necessary, and ensuring that only authorized users can access them.

(3) Forensics: The framework includes a forensic component to aid in the investigation of security incidents. This component uses digital forensics techniques to gather evidence of an attack and reconstruct the sequence of events leading up to the attack.

(4) Overall, the proposed framework aims to increase the security of networked medical devices and reduce the risk of cyber attacks that could compromise patient safety and privacy.

To mitigate the same issue, in case of device loss/theft, Bhatia et al. [148] proposed a soft computing approach for mitigating real-time abuse in IoT systems by detecting and predicting anomalies. The proposed approach uses a hybrid model that combines an online clustering algorithm with a time-series prediction model. The online clustering algorithm is used to identify anomalous data points in real time, while the time-series prediction model is used to predict future values of the IoT data. Since these devices hold sensitive data, they need a strong authentication mechanism to make them more secure. One possible mitigation approach is continuous authentication, which is possible in the case of skin-attached medical wearable equipment.

Zhao et al. [149] proposed a continuous authentication system based on cardiac biometrics measured from wrist-worn wearables. This approach aims to address the limitations of traditional authentication methods by using a biometric that is difficult to forge or steal and can be watched continuously without causing inconvenience to the user. The proposed system uses machine-learning algorithms to classify the users' cardiac biometrics and authenticate the user in real time. Continuous biometric authentication methods, while effective, raise concerns about user convenience and the accuracy of measurements under varying physical conditions. Gulhane et al. [150] introduced a novel risk assessment framework for VR learning environments, employing attack trees to compute a risk score for diverse threats within VRLEs.

In pursuit of striking a balance between privacy and data access, Fang et al. [151] introduced a **fine-grained privacy-preserving access control architecture (FPAS)** tailored for smartwatches. Their approach utilizes an **identity-based authentication scheme** leveraging cryptography, coupled with the segmentation of data requesters based on distinct attributes.

3.6.3. Open Problems

Wearable devices, often worn near the human body, store a wealth of user information, including personal sensitive biomedical data, heart rate, sleep patterns, and even user behavior. The leakage of such sensitive information represents a significant threat to user privacy and well-being, potentially leading to identity theft or manipulation of health records. Addressing this critical issue should be at the forefront for researchers, particularly in developing a robust data encryption method and secure communication protocols for wearable devices.

3.7. Category 7: IoT in Smart Retail and Supply Chain.

3.7.1. Security Challenges

The burgeoning adoption of IoT in the retail sector, projected to reach a staggering $94 billion by 2025, presents a new wave of security challenges [152]. As retailers start integrating smart systems like contactless point of sale (POS), systems, mobile transactions, or smart shelves to enhance customer experience and business agility [153,154], these interconnected devices create a complex attack surface for malicious actors. The security risks in the retail IoT (RIoT) are multifaceted. **Data security** has been the prime concern as retailers face the rising threat of complex cyber attacks and the potential for data breaches. Such breaches can lead to significant brand damage and customer loyalty loss [155]. Major retail companies' utilization of payment platforms like Apple Pay and Google Pay is causing concerns about cyber attacks and potential financial losses. It is reported that since 2005, retailers have seen over 10,000 data breaches, mainly due to flaws and vulnerabilities in the payment system [156].

POS systems often involve multiple components, including external hardware, software, and cloud-based services. Security vulnerabilities in such intricate networks can explode at any instance, and thus, it is very cumbersome to tackle RIoT security on a device-by-device basis. Cybercriminals have numerous opportunities to exploit retail systems, whether it is at the vendor's source or during on-site technology deployment. Exploiting a security issue in the software used on POS devices or the cloud server could allow the deployment of malware or infected software. This malicious software cannot only damage the retail system but can also steal customer financial information, leading to significant financial loss and reputational damage to the brand of the company. While RIoT can enhance the consumer–brand relationship through features like purchase history tracking, customers might feel hesitant to engage in such technologies if they fear their data are not secure. A data breach exposing customer purchase history could lead to financial losses and erode customer trust. Unreliable code and/or software of RIoT introduces an additional layer of security risk, as attackers can easily manipulate the code to access sensitive information. The other security threat is the surveillance system of RIoT. RIoT often utilizes **customer tracking technologies**, raising privacy concerns. While tracking customer movements and purchasing habits can be beneficial for targeted marketing/advertisements, it is crucial to prioritize user privacy by ensuring data collection security, transparency, and compliance with regulations like general data protection regulation (GDPR) or country-specific data protection laws [157]. We know that RIoT tracks customers' movements and purchasing habits deliberately, as purchasing behavior correlated with consumers' movements can reveal extremely private habits. Tracking technologies like Wi-Fi logging and biometric imaging pose significant privacy risks, as they may create full behavioral profiles of consumers and could be misused for targeted marketing or discriminatory pricing [158] **Ransomware attacks** are also prevailing in the supply chain networks due to overlapping security systems. Ransomware attacks on supply chains exploit interdependencies, causing cascading disruptions that amplify financial losses and operational delays across upstream and downstream partners. The ransom is lowest for a hub and spoke network and highest for a line network. For example, the attack on Kojima Industries disrupted Toyota's production, showcasing the vulnerability of interconnected systems and the critical need for coordinated cybersecurity strategies [159]. **Supply chain attacks** are adversarial attacks on supply chain methods.

- In supply chain systems, several IoTs act as network-connected sensors that may be part of cyber–physical systems. Hence, each IoT is being treated as a new door for adversaries [160].

- It is conceivable that this could lead to supply chain attacks, as the same type of attack that caused a single disruption in production could potentially be employed to impact and disrupt an entire supply chain simultaneously.

Retail IoT systems are also vulnerable to DDoS attacks, which can disrupt critical systems such as POS terminals and inventory management systems. These attacks can also result in financial losses and damage to retailers' reputations. The short lifespan of IoT devices introduces a significant security challenge [27]. Once these devices meet their end-of-life and are no longer supported with security updates, they become vulnerable to exploitation. Intruders can potentially compromise outdated devices to gain access to sensitive data within a large supply chain, leading to confidentiality breaches, integrity, or availability of the entire system.

3.7.2. Mitigation Approaches

The new era of finding security solutions is inclining toward machine learning, AI, Blockchain, etc. Fog computing, ML, and AI can all play important roles in enhancing the security of retail IoT devices and systems. Additionally, homomorphic encryption (HE) provides an innovative solution to enhance the security of Retail IoT systems by enabling computations on encrypted data without decrypting them. This ensures that sensitive customer data remain secure even during processing. For instance, **Fully Homomorphic Encryption (FHE)**, a robust subset of HE, allows complete arithmetic operations on encrypted data, thereby reducing the risk of exposure to data breaches [161].

Fog computing involves processing data at the network's edge, closer to the devices generating the data, rather than sending all the data to the cloud for processing. This approach can improve security by reducing the amount of sensitive data that needs to be transmitted over the network, minimizing the potential attack surface for malicious actors. Additionally, fog computing allows for real-time analysis of data, enabling tasks like monitoring devices' behavior for anomalies, triggering alerts for suspicious activities, and even blocking unauthorized access attempts. The rapidly evolving landscape of RIoT security demands innovative solutions. Fog computing brings a powerful solution to enhance security, particularly within supply chains. In this direction, Musa and Vidyasankar et al. [162] proposed a **fog computing framework** that integrates edge/cloud-computing and IoT to real-time monitoring and analysis of supply chain data. This framework also includes a security layer to enhance the efficiency and security of BlackBerry's sensitive information. To address the DDoS attack in RIoT systems, Brasilino et al. [163] proposed a custom hardware solution. The solution consists of two main components:

- A hardware module that performs the actual DDoS mitigation and,
- A software framework that orchestrates the hardware module and provides an interface for configuring and managing the mitigation process.

The proposed custom hardware is designed to be placed between the IoT devices and the network. The integration of IoT technologies into retail oil outlets (ROO) presents a mix of opportunities and challenges. While technologies like cloud-based IoT offer numerous advantages for streamlining operations and gathering valuable data, it also introduces new security concerns. To address this concern, Das et al. [164] propose a model for ROO by incorporating "data security" into the existent framework of technology, organization, and environment within the IoT ecosystem. This model is effective in providing a holistic approach to secure data throughput in the lifecycle of ROO operation.

To further strengthen Das's data-centric model, Mohanta et al. [165] proposed the use of ML, AI, and Blockchain technology as potential solutions. Specifically, these technologies can be used for: Intrusion detection and prevention: machine learning and AI are being used to analyze network traffic and identify anomalous behavior that may indicate a

security breach. As discussed earlier, securing device identity is paramount. Blockchain technology excels in creating a secure and decentralized system for authenticating IoT devices and controlling access to sensitive data. This ensures that only authorized devices can connect to the internet, alleviating the risk of unauthorized access. Data encryption and privacy protection: to encrypt data and protect the privacy of sensitive information, AI and ML are being used extensively. Threat intelligence and incident response: machine learning and AI can analyze data security and provide real-time insights into emerging threats, allowing for more effective incident response.

3.7.3. Open Problems

A major challenge facing RIoT security revolves around financial transactions. Many of these transactions involving IoT devices rely on personal information stored in the cloud, thereby introducing an additional vulnerability susceptible to potential malicious attacks. These inherent vulnerabilities necessitate robust security measures to safeguard financial data and transactions within the RIoT ecosystem.

3.8. Category 8: IoT in Agriculture

3.8.1. Security Challenges

In the facets of changing climate and exploding global population, smart devices are emerging as an essential tool for precision agriculture [166,167]. However, integrating the Agriculture Internet of Things (AIoT) and cloud computing promises enhanced crop production through cost reduction, efficient monitoring of crops, and maintenance. It also introduces security concerns and major cyber attacks on critical agriculture infrastructure [168–170]. The most common examples of cloud-based IoT applications in agriculture are (1) smart sensor-based IoT devices for monitoring crops, soil, fields, livestock, storage facilities, or generally any necessary factor that influences agriculture production [171,172]; (2) smart IoT agriculture vehicles, drones, autonomous robots, and actuators (e.g., DroneSeed, SenseFly, SoilCares [173]); (3) smart greenhouse and hydroponics [174]; (4) for data analytics, data visualization, and data management systems in agriculture; (5) predictive modeling and planning; (6) precision agriculture using IoT [167,175].

The rapid evolution of IoT, communication technology, and digitization introduces new security risks in AIoT. In agriculture, interconnected AIoT systems collect and analyze data, creating vulnerabilities that can be exploited, leading to significant disruption [176,177]. Mori et al. [178] have further explored these security concerns in detail, highlighting the complexity of securing a secure environment with multiple interconnected IoT devices. AIoT relies on multiple interconnected sensors, so compromising one device can create a domino effect, making others vulnerable. When interconnected devices such as sensors are compromised, the disruptions can propagate through the entire network, affecting water distribution, sensor readings, and automated equipment. This can significantly hinder agricultural productivity and expose unforeseen vulnerabilities in supply chains reliant on stable operations. Data tampering is another issue where hackers can access and alter data transmitted to weather stations or cloud servers, leading to inaccurate analysis and poor decision-making by farmers.

AIoT security vulnerabilities manifest across all layers of the IoT framework. The first application layer, where farmers connect with IoT devices, has a high risk of data theft [179]. The layer experiences a range of security challenges, including **data theft, access control sniffing attacks, and service interruption attacks**. These threats can potentially disrupt the delivery of IoT services to farmers [180,181]. Security vulnerabilities with AIoT have a cascading effect, impacting not only IoT–farmer relationships but also retailers–stakeholders throughout the agriculture supply chain. Attacks targeting the application layer can po-

tentially disrupt communication and data access for all connected individuals (farmers, retailers, stakeholders), jeopardizing trust and collaboration. The security vulnerabilities in the AIoT framework extend beyond the application layer.

The middleware layer, acting as an intermediary between hardware and applications, presents significant security risks, including **MITM, SQL injection, signature wrapping, cloud malware injection, and flooding attacks.** These attacks compromise device data, disrupt access control mechanisms, and may hurt the farmer's decision-making abilities. Thus, it is of paramount importance to explore the security of these devices, ensure process and access control, and maintain the integrity of data analysis [182,183].

The cloud server connecting AIoT devices to the internet is a critical vulnerability point, susceptible to phishing, access, DDoS, data transit, and routing attacks [184].

This layer is responsible for conducting communication between device-to-device, device-to-cloud, device-to-gateway, and back-end data-sharing. A disruption at this layer could result in the device and service becoming non-functional. Moreover, if the data exchanged between IoT devices and the cloud are transmitted in plain-text without encryption, it can raise privacy concerns that impact both the IoT device and the farmers' data.

3.8.2. Mitigation Approaches

Due to the complexity of the smart agriculture environment, AIoT is vulnerable to **intrusion attacks**. These attacks involve unauthorized access to a farm's IoT network, compromising sensitive data related to crop production, livestock monitoring, or equipment management. ML can play a vital role in mitigating these attacks. Raghuvanshi et al. [185] proposed an intrusion detection mechanism using machine-learning techniques, designed to detect abnormal behavior in the smart irrigation system, which could be indicative of a security breach. Through the utilization of machine-learning algorithms for intrusion detection, the system can evolve to address emerging threats and enhance its accuracy progressively. Building on this, federated learning frameworks offer a decentralized approach to training machine-learning models across multiple devices. This approach enables collaborative learning for applications like disease detection and yield forecasting while preserving sensitive agricultural data on local devices [186]. As machine learning continues to advance, deep learning emerges as a modern tool that offers a secure and privacy-preserving framework for smart agriculture. One such example is the **Secured Privacy-Preserving Framework (SP2F)** proposed by Kumar et al. [187]. The proposed framework is designed to protect the privacy and security of data collected by UAVs while still allowing for efficient and effective data analysis. To address the risks posed by data tampering, integrating anomaly detection algorithms with real-time monitoring systems can help identify irregularities in weather or soil data. Additionally, deploying redundant sensors and implementing cross-verification mechanisms can maintain data accuracy and reliability, even when some systems are compromised [188].

Another approach for preserving privacy in smart agriculture involves a data aggregation scheme. Song et al. [189] proposed a scheme that uses the **ElGamal Cryptosystem** to enable secure aggregation of data while protecting individual data points.

- The proposed scheme has been rigorously analyzed and designed to particularly benefit farmers to share and analyze their combined data sets without compromising the privacy of the sensor reading.
- This approach is capable of solving the privacy-preserving issue not only in smart agriculture scenarios but also in the other applications of IoT.

Furthermore, Zhou et al. [190] have proposed a **complementary privacy-preserving solution**, specifically designed for fog-based agricultural IoT systems.

- The scheme leverages secure multi-party computation techniques, allowing data owners to query the maximum value within a specific range without disclosing any sensitive information about their data to the fog nodes.
- The proposed scheme is particularly useful when analyzing aggregate data at the fog, which can help to minimize computation and communication overhead while ensuring data privacy [190].

While privacy preservation is crucial, another security challenge exists in smart agriculture, another approach involves a framework designed to detect anomalies in data collected from various sources within a smart farming system while preserving the privacy of sensitive data using homomorphic encryption techniques [191].

Looking beyond privacy, Kumar et al. [192] proposed a deep privacy-encoding-based federated learning framework (PEFL) to address privacy concerns associated with federated learning in smart agriculture systems by utilizing a deep privacy-encoding mechanism. Federated learning allows distributed training on devices, further minimizing the security risk associated with data sharing. Minimizing the risk of cascading failures in interconnected systems can be achieved through decentralized approaches, such as edge computing and Blockchain-based coordination. These methods help contain compromised devices and prevent disruptions from spreading across the network [193]. Anidu and Dara et al. [194] believe that standardization could be a potential solution for interoperability and consistency issues in a smart agriculture environment, whereas the Blockchain and distributed ledger technology could help in mitigating data integrity and data confidentiality issues and thus making the data storage system more secure than before.

Security monitoring is crucial to ensure the safety of smart farming. Modern technology can avail better security solutions for vulnerabilities within AIoT. One such example is the cloud-based security monitoring framework proposed by Chaganti et al. [195]. This framework effectively monitors device status and sensor data for anomalies, potentially identifying unauthorized access or other security breaches. Additionally, it utilizes a Blockchain-based smart contract application to securely store information about identified security anomalies. This allows for proactive mitigation for other similar attacks targeting other farms within the network.

3.8.3. Open Problems

AIoT devices are often resource-constrained, with limitations in processing power, memory, and battery life. These constraints make it challenging to implement robust security measures, leaving them widely vulnerable to unauthorized access and data breaches. These vulnerabilities could compromise sensitive agricultural information like crop yields, weather data, and farm operations. Human factors such as negligence, weak passwords, or poor security practices by farm personnel further complicate security issues. To effectively secure AIoT devices, lightweight security protocols specifically designed for resource-constrained devices are crucial. While designing these protocols, care must be taken to balance the need for strong security while still preserving the user-friendly experience for farmers, considering the inherent device limitations.

3.9. Category 9: IoT in Smart Grids

3.9.1. Security Challenges

As demand for sustainable energy grows, smart grid technologies are attracting attention for their efficient energy distribution, improved grid reliability, and integration of renewable sources [196]. Some examples of IoT in smart grids include smart switches, smart metering systems [197], smart thermostats [198], smart batteries [199], etc. Smart grid IoT devices, which are used to monitor, control, and optimize the distribution of

energy across the power grid, are increasingly being integrated with cloud-based services to enable remote management and analysis. While cloud-based smart grid systems offer numerous benefits, they also pose several security risks that need to be addressed. Some of the security issues that arise in cloud-based smart grid IoT devices are data privacy issues, malware attacks issue, DDoS attacks, standardization, transparency issues, etc.

Smart grid systems generate huge amounts of sensitive and private data, including customer personal information, energy usage patterns, and grid performance data which are vulnerable to leaks. These data need to be protected from unauthorized access, theft, or misuse [200]. One particular security threat in the smart grid is a **false data injection attack.** In this attack, the attacker injects false or malicious data into the system to disrupt its operation or steal information. In a smart grid, IoT devices are used to monitor and control the flow of electricity, and attackers can exploit vulnerabilities in these devices to inject false data. These false data can then cause the smart grid to malfunction or behave in unexpected ways, potentially leading to power outages or other disruptions. These are just some concerning examples of the security risks associated with cloud-based smart grids. Addressing these issues is crucial for ensuring the reliable and secure operation of the smart grid system.

Another security threat to the smart grid is a DDoS attack. Various types of DDoS attacks can be directed at different components of the smart grid, including meters, communication networks, and control systems. Successful DDoS attacks on the smart grid infrastructure can have severe consequences, potentially resulting in power outages, data loss, and financial damages [201]. Cloud-based smart grid systems are susceptible to various cyber attacks that can disrupt operations or compromise sensitive data. Malicious software malware and DDoS are major concerns for this category. Malware can be introduced through compromised IoT devices or phishing attacks on cloud service providers [202]. DDoS attacks can be used by attackers to overload cloud-based smart grid systems, leading to system crashes or unavailability. This can lead to disruptions in energy distribution and other critical services [203].

Additional challenges exist beyond cyber attacks and DDoS attacks. Insider threats can arise if unauthorized personnel misuse this private information for personal gain, potentially engaging in illegal activities [204].

A lack of standardization in cloud-based smart grid systems can create vulnerabilities, as different vendors may have different security protocols or use different data formats that may not be compatible with each other. Lack of transparency in cloud-based smart grid systems poses other vulnerabilities, as users may not have full visibility into the data being collected, processed, or shared. Smart batteries are also prone to unauthorized access to battery data and control systems. The attackers can exploit vulnerabilities in the battery's software and hardware and could gain access to sensitive information. This could possibly result in battery failure, data theft, or other security issues. The smart grid collects a large amount of data from consumers, which can include sensitive information such as energy consumption patterns and personal preferences. Attackers can exploit these data further to breach consumers' privacy.

3.9.2. Mitigation Approaches

The security of the smart grid necessitates a multi-layered approach that addresses vulnerabilities across cloud-based systems and individual components. Robust authentication mechanisms, data encryption, and intrusion detection systems can enhance cloud security. The integration of post-quantum cryptography (PQC) to secure the smart grids can be a future-proof solution. With quantum computing poised to undermine traditional crypto-

graphic methods, PQC algorithms—resilient to quantum attacks—ensure the long-term security of communications and data within smart grid infrastructures [205].

Regular security audits, employee training, and incident response plans are also important to ensure the security of these systems. To mitigate these security concerns, manufacturers of smart batteries should implement strong encryption and authentication measures to protect data and communication channels. They should also incorporate tamper-evident features to prevent physical attacks on the battery. Moreover, routine firmware updates can help mitigate numerous security vulnerabilities and enhance the security of both the battery's software and hardware.

Security vulnerabilities in the smart grid can be life-threatening, leading to a loss of critical services, physical damage to infrastructure, and potential safety hazards for individuals. Early detection and mitigation are of the utmost importance, as vulnerabilities can disrupt critical services, damage infrastructure, and pose potential safety hazards. Researchers are exploring various approaches to mitigate these risks. For instance, Yılmaz and Uludag [206] proposed a framework for **anomaly detection and attack recognition** that leverages data from various sources, including IoT devices, network traffic, and system logs. The mitigation and response mechanism involves isolating the affected devices and shutting down the affected systems to prevent further damage. To address the cybersecurity issue in smart grids, Muyeen's group [207] suggested the use of machine learning to tackle the issue. They acknowledged that machine learning can be used for cybersecurity in smart grids, including intrusion detection, threat intelligence, anomaly detection, and risk assessment.

The smart grid is vulnerable to both faults and cyber attacks, and a comprehensive security scheme is necessary to ensure the reliable and secure operation of the grid. There should be multi-layer security to mitigate vulnerabilities in the smart grid against faults and cyber attacks. Chen et al. [208] proposed a three-layer security scheme that includes the physical layer, network layer, and application layer security. A **distributed trust management system (DTMS)** can be used to mitigate false data injection attacks (FDAs). FDAs inject malicious data that can evade traditional detection methods, thereby threatening grid reliability and causing major operational challenges [209] The DTMS consists of a set of trust nodes that are responsible for verifying the data received from the sensors and measurement devices of the smart grid. The trust nodes use a distributed consensus algorithm to reach a consensus on the correctness of the data [210]. However, DTMS has limitations, including the requirement for extensive collaboration among stakeholders, which may not always be feasible.

To address the privacy breach, the **smart generative adversarial network (GAN)** can be used to obfuscate consumer data. GAN generates synthetic data that are similar to real data but do not reveal the consumers' actual information. The synthetic data are then used for analysis and decision-making, while the real data are obfuscated to protect the privacy of the consumers [211]. To mitigate cyber and physical attacks, big data and AI technologies can be used to analyze and predict the security risks in the smart grid. To mitigate DDoS attacks in smart grids, various techniques like intrusion detection systems, firewalls, and load balancing mechanisms can be used. One such approach has been proposed by Chehri et al. [212], a framework that consists of four phases: data collection, data preprocessing, risk modeling, and risk evaluation. In the risk modeling phase of the four phases, diverse AI techniques like machine learning and deep learning are employed to model security risks within the smart grid.

3.9.3. Open Problems

The global shift to smart grids offers significant benefits in energy integration and management, as seen in Germany's IoT-enabled grid optimizing renewable energy. However, this transition introduces security risks. As many capitals aim for IoT-based smart grids to achieve net-zero goals by 2050, the increase in devices heightens security concerns.

Key future challenges include developing robust security frameworks, ensuring data integrity and privacy, and establishing standardized protocols for smart grid technologies.

3.10. Category 10: Cloud-Based IoT in Aviation

3.10.1. Security Challenges

Cloud-based IoT solutions are transforming aviation by streamlining data collection, processing, and analysis in the industry. Some of the key applications of cloud-based aviation IoT are Smart Airport [213], predictive maintenance [214], improving customer satisfaction [215], safety management [216], improving the overall performance by reducing emissions [217], luggage management [218], in-flight entertainment systems [219,220], etc. In addressing security challenges within this category, **data security** emerges as a foremost concern. Given that cloud-based Aviation IoT systems extensively depend on data collection and transmission, safeguarding the integrity and confidentiality of these data is of prime concern. Any data breach has the potential to result in harm to aircraft, passengers, and the airline's reputation [221].

A recent study by Aboti [222] discusses escalating security challenges and threats faced by smart airports due to the integration of IIoT and the increased use of smart devices. The integration has opened doors for vulnerabilities like malware, cyber attacks, and insider threats. The authors emphasize the importance of implementing robust cybersecurity governance in smart airports to protect against cyber threats and enhance operational practice. Cho et al. [223] provided a case study highlighting the importance of cybersecurity in commercial aviation. The main security issue discussed by Ukwandu et al. [224] is the vulnerability of aviation infrastructure to cyber attacks, particularly from Advanced Persistent Threat (APT) groups that operate in collaboration with a particular state actor to steal intellectual property and intelligence to advance their domestic aerospace capabilities as well as monitor, infiltrate, and subvert other sovereign nations' capabilities.

Lazaro's group [225] conducted a study by combining interviews with airport security personnel and a survey of airport users to gather data on the cyber security risks and vulnerabilities of Spanish airports. The study identified several cyber security risks, including inadequate user authentication measures, vulnerabilities in airport software systems, and the use of insecure communication channels. In the context of aviation cyber security, the use of Electronic Flight Bags (EFBs) adds a layer of risk, as unauthorized access to EFB servers could potentially compromise the safety and security of aircraft operations.

Hackers exploit vulnerabilities in the remote desktop protocol or use **phishing attacks** to steal login credentials and gain unauthorized access to aviation IoT systems. This unauthorized access can lead to a variety of negative consequences, such as stealing sensitive data, causing equipment malfunctions, and compromising the safety of passengers and crew. Considering the significant volume of data collected by IoT devices in the aviation industry, ensuring the privacy and confidentiality of these data becomes a major concern. Additionally, the complex environment of connected IoT devices in aviation increases vulnerability to cybersecurity threats. In the worst scenario, hackers might manipulate or disable critical equipment, leading to malfunction and potential hazards. Overall, robust security measures must be implemented to mitigate these risks and protect the aviation sector from potential cyber attacks.

3.10.2. Mitigation Approaches

The aviation industry is facing a growing challenge from cyber attacks. To counter this challenge, researchers are exploring several approaches. One such approach has been proposed by Sam Adhikar [226] that leverages 5G and intelligent cyber defense mechanisms to enhance the security of aviation systems, focusing on high-speed data transfer and advanced threat detection.

Airports have robust security measures, such as the use of encryption technologies, regular security audits, and employee training programs. Moreover, **Blockchain-based decentralized identity management systems** can significantly enhance authentication mechanisms. It will enhance authentication in aviation IoT by decentralizing identity repositories, reducing single points of failure, and strengthening security through improved transparency and traceability [227].

In a study, Belkens's group's suggested approach consists of three main components

(1)   A 5G-enabled communication network that provides high-speed, low-latency connectivity between aviation systems and enables real-time threat detection and response;

(2)   An intelligent cyber defense system that uses AI and ML algorithms to detect and mitigate cyber threats in real time; and

(3)   A set of best practices and guidelines for the implementation and operation of the cybersecurity framework [224].

In another measure, Lazaro et al. [225] recommended that a proactive and collaborative approach to cybersecurity is essential to guarantee the safety and security of Spanish airports and the well-being of passengers. In another study, Zkik et al. [228] proposed a secure and reliable model for the traceability of records in the airline supply chain using Blockchain and machine-learning technologies. The model is designed to enhance the efficiency and security of the supply chain by providing real-time tracking and monitoring of records related to cargo and other goods. ML and AI could be better alternatives to finding solutions for security attacks caused by electronic flight bags.

Bitton et al. [229] proposed a system that utilizes a combination of feature engineering and machine-learning algorithms to detect and classify intrusions in real time. The study focuses specifically on securing remote desktop connections, which are a common attack vector for cybercriminals seeking to gain unauthorized access to EFB servers. In addition to the general security measures, specific security measures need to be taken for IoT devices in the aviation sector. Such measures encompass adopting secure communication protocols, enforcing robust authentication and access control, conducting routine security audits, maintaining up-to-date firmware, and encrypting sensitive data. Through the implementation of these security measures, the aviation sector can mitigate risks linked with IoT devices, thereby guaranteeing the safe and secure integration of this technology.

3.10.3. Open Problems

Despite advancements in security, aviation IoT continues to face significant challenges, including data security risks like passenger data breaches and vulnerabilities to cyber threats such as malware and phishing attacks. Malware can compromise, steal data, and disrupt operations, while phishing can deceive passengers into revealing sensitive information, leading to financial losses. These issues threaten system integrity and pose substantial risks. To enhance the safety and security of aviation IoT systems, implementing robust security measures like encryption, access control, regular audits, and comprehensive employee training on cyber threats is essential.

4. The Way Forward: In Search of Uniform Solutions for All Security Challenges

The rapid growth of IoT devices highlights the urgent need for global cybersecurity measures. Consequently, 2024 emerges as a pivotal juncture prompting governments to scrutinize advancements in laws and regulations [230]. To accomplish this goal, numerous nations have developed distinct regulatory standards aimed at enhancing the security of IoT. For instance, the European Union introduced the Cybersecurity Act and Cyber Resilience Act to bolster cybersecurity throughout the EU, complementing existing legislation such as the GDPR and the Network and Information Security Directive [230,231]. Likewise, in the United States, IoT regulatory standards encompass the Federal Trade Commission Act, the Cybersecurity Information Sharing Act, and COPPA [231]. Other countries are also subject to their own nation-specific laws, with some currently in the process of formulating regulations. Despite the nation-specific IoT regulations, there is a universal desire for a standardized security solution along with some similar ongoing work [232]. Addressing the myriad of security and privacy challenges in cloud-based IoT and creating a one-size-fits-all security solution for the diverse security and privacy challenges in cloud-based IoT is a complex task (RQ3). Various ongoing industrial collaborations are underway to achieve this goal [233]. Thus, the solution to RQ3 is feasible but remains a challenging task to implement across all categories of IoT. The rationale behind this lies in the distinct characteristics of each category of traditional and cloud-based IoT devices. For instance, consumer-oriented devices can easily scale up to accommodate more hardware resources, while medical wearable devices must remain compact and portable. Consequently, security solutions must be tailored to the specific features of each category. In our section on mitigation approaches, we delve into potential solutions, recognizing the need for category-specific security measures. Nonetheless, we put forth an optimal approach aimed at mitigating the security issue to a certain extent. In the realm of IoT devices intended for consumer use, a complex ecosystem involving multiple third parties is typically at play, which can generally be categorized into three levels: the manufacturer (responsible for hardware components like sensors, memory cards, etc.), third-party services (involving tasks such as device code development, natural language processing, etc), and cloud services (facilitating internet connectivity, communication with end-users, etc.). We advocate for the implementation of a multi-level protocol verification framework tailored for IoT, emphasizing rigorous security checks across manufacturing, third-party services, and cloud service levels. This approach ensures a structured and consistent security evaluation process. To cater to IoT categories with higher resource constraints, such as medical wearables or AIoT, we propose integrating adaptive verification systems driven by machine learning. These systems can dynamically adjust security measures based on real-time device usage patterns, enabling scalable and efficient implementation. For large-scale IoT ecosystems, AI-driven modular verification systems can adapt security protocols based on device complexity. For instance, consumer-oriented IoT devices may rely on more scalable solutions like cloud-based security checks, while life-critical IoT devices, such as healthcare IoT or autonomous vehicles, would require more intensive localized verifications to ensure real-time safety and data integrity. Additionally, incentivizing manufacturers and cloud providers to adopt these frameworks through compliance rewards or certifications could accelerate adoption. Hence, we believe this standardized verification mechanism has the potential to be a significant milestone in addressing security concerns, particularly in the context of life-critical IoT devices.

5. Limitations

Although this paper categorizes cloud-based IoT into ten distinct types, we recognize that the field is continuously evolving, and additional categories or hybrid domains may emerge over time. To address this dynamic nature, the proposed framework is intentionally designed to be flexible and adaptable, providing a robust foundation for future research and development in enhancing the security of cloud-based IoT systems.

6. Conclusions

This paper introduces a novel method to analyze IoT security by categorizing devices into ten distinct areas, each with unique challenges (as shown in Table 2). The goal is to identify and address the security issues of each category and explore existing solutions, highlighting areas for future research when solutions are lacking. This study also notes that some IoT devices may not rely on cloud computing and possess their own security challenges, which are expected to increase as they integrate more with cloud services. This paper discusses the added risks, such as data breaches and DDoS attacks from cloud integration, especially for resource-limited devices like wearables, emphasizing the importance of proactive security measures in IoT design and deployment. Additionally, the possibility of implementing standardized security solutions across all categories is explored to enhance overall IoT security and protect user data.

Table 2. Short summary table for each category.

Category	Issues	Mitigations	Use Cases	Ref.
Consumer-oriented IoT	VSA, third-party criticality, interoperability issue, MITM, DDoS attack, flash memory issue, data leakages, debugging interface issue, hardcoded-password issue, authentication issue, data collection issue.	SkillFence, cryptosystem, SDN, flow filtering, honeypot technique, rate limiting approach, MTD, Traceback, LOKI.	Amazon's Alexa, Google Assistant, Samsung's SmartThings, web camera*, Nest smoke alarm.	[7,14,23,29,36–77]
Children's IoT	Eavesdropping issue, camera privacy issue, weak encryption, access control issue, POST tokens issue, jamming attack, plain-text API issue, personal information leak, authentication bypass issues, direct browsing issue, privilege escalation problem, backdoor credential leaks, remote cell access issue, unlock protected passwords issue, UART issue, authentication issue, DDoS attack.	Built-in security mechanism.	Hydrogen tracker, smart robots*, smart dolls*, hello barbie doll, BB8, baby application monitor.	[5,8,16,30,78–87]
Healthcare IoT	Encryption issues, dictionary attacks for passwords, weak passwords, memory card issues, plaint-text API issues, DDoS attacks, data integrity, data confidentiality, data availability issues, replay, MITM, impersonation, and privileged-insider attacks.	Anonymization techniques, Blockchain mechanisms, bulwark, decision tree algorithm, ML-based healthGuard, cryptographic techniques, GHOSTDAG, deep learning concepts.	HRPM*, pulse oximeter*, DCT*, glucometers*, fire safety and security monitoring, indoor localization for healthcare facilities.	[6,11,88–90,92–101,103–110]

Table 2. *Cont.*

Category	Issues	Mitigations	Use Cases	Ref.
Industrial IoT	Insufficient industrial hardware data protection, hardware memory dump, unprotected hardware interface, analog signal processing issue, DDoS, and device infiltration.	TPMs, STC scheme, VFNs, FLEAM.	Temperature/pressure sensors*, proximity server, smart meter, temperature-based control system*, cloud-based video surveillance systems.	[15,53,111–128]
Smart Vehicle	Privacy threat, data authenticity attack, availability attack, Sybil attack, GPS deception attack, authentication attack, masquerading attack, wormhole attack, replay attack, data injection attack.	Secure software development practice, secure boot processes, hardware-based encryption methods, AI and ML, Blockchain-based architecture, and cloud-based sandboxing approach.	Smart vehicles.	[31,129–132,134–137,234]
Wearable IoT	CIA triad, DDoS attacks, data leakage, MITM attacks, phishing attacks, eavesdropping, side-channel attacks, compromised attacks, personal information leaks in case of theft, hardcoded password issues, code injection issues, unsecured API issues, web application vulnerability issues, and lack of encryption in communication.	Out-of-band biometrics authentication (OOB BA), attack-Surface Reduction by Design, soft computing approach, continuous authentication, attack trees, FPAS.	Smart cloths*, smart wrist-wear, smart jewelry, smart foot wear*, smart eye wear, sensor patches*, medical wearable devices.	[11,138–151]
Smart Retail	Cyber breach, personal behavior breach, financial information leaking.	ML, AI, and Blockchain. Fog computing, cloud computing, custom hardware solutions, edge computing.	Contactless POS system, mobile transactions, or smart shelves*, IoT-based fruits and vegetable sales system*.	[27,152–157,159,160,162–165]
Agriculture IoT	Sensor hacked, data theft, access control sniffing attacks and service interrupt attacks, MITM, SQL injection attacks, signature wrapping attacks, cloud malware injection attacks, flooding attacks, phishing attacks, access attacks, DDoS attacks, data transit attacks, and routing attacks.	Intrusion detection mechanism using ML, data aggregation scheme, SP2F, multi-party computation techniques, homomorphic encryption technique, FPDP PEFL.	Ag vehicles, concept cars*, drones, smart sprinklers, lights, coolers, heaters*, DroneSeed, SenseFly SoilCares, moisture sensor*, allMETEO, Smart Elements, Pycno, CropX, Mothive, FarmappGrowlink, GreenIQ, Arable, Semios, SCR and Cowlar, attitude model.	[166–185,187,189–192,194,195]
Smart Grid	Data privacy issues, malware attacks issue, DDos attacks, standardization issues, transparency issues, false data injection attacks, unauthorized access, insider threats.	Strong authentication mechanisms, data encryption, intrusion detection systems, regular security audits, employee training, incident response plans, anomaly detection and attack recognition, DTMS, GAN, big data and AI technologies, firewalls, and load balancing mechanisms.	Smart switches and sensors*, smart metering systems, smart inverters, grid sensors*, smart thermostats, smart batteries.	[196–204,206–208,210–212]

Table 2. *Cont.*

Category	Issues	Mitigations	Use Cases	Ref.
Aviation IoT	Data security, malware, cyber attacks, inadequate user authentication, insider threats, vulnerabilities in airport software systems, insecure communication channels, unauthorized access to EFB servers, equipment malfunctions, and compromising the safety of passengers and crew.	AI, Blockchain, data encryption, regular security audits, employee training programs, feature engineering, ML, secure communication protocols, strong authentication, and access control measures.	Predictive maintenance, monitoring aircraft performance and optimization operations, smart baggage, smart airport, safety management*, flyers experience, and in-flight entertainment system.	[213–226,228,229]

Penultimately, we envision an ideal world where responsible citizens take proactive measures to safeguard their digital lives. By actively updating device passwords and firmware and limiting the sharing of private data, individuals play a pivotal role in addressing security and privacy concerns. This collective effort towards adopting best practices empowers us to create a safer and more secure digital environment for all.

Institutional Review Board Statement: This study did not collect any data.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kumar, S.; Tiwari, P.; Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *J. Big Data* **2019**, *6*, 1–21. [CrossRef]
2. Kamal, M.; Aljohani, A.; Alanazi, E. IoT meets COVID-19: Status, Challenges, and Opportunities. *arXiv* **2020**, arXiv:2007.12268.
3. Tabrizi, S.S.; Ibrahim, D. A Review on Cloud Computing and Internet of Things. *Int. J. Comput. Inf. Eng.* **2017**, *11*, 493–498.
4. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. Sok: Security evaluation of home-based iot deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 13–23 May 2019; pp. 1362–1380.
5. Apthorpe, N.; Reisman, D.; Feamster, N. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv* **2017**, arXiv:1705.06805.
6. Bradley, C.; El-Tawab, S.; Heydari, M.H. Security analysis of an IoT system used for indoor localization in healthcare facilities. In Proceedings of the 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 27 April 2018; pp. 147–152.
7. Celik, Z.B.; McDaniel, P.; Tan, G. Soteria: Automated {IoT} Safety and Security Analysis. In Proceedings of the 2018 USENIX Annual Technical Conference (USENIX ATC 18), Boston, MA, USA, 11–13 July 2018; pp. 147–158.
8. Chu, G.; Apthorpe, N.; Feamster, N. Security and privacy analyses of internet of things children's toys. *IEEE Internet Things J.* **2018**, *6*, 978–985. [CrossRef]
9. Denning, T.; Kohno, T.; Levy, H.M. Computer security and the modern home. *Commun. ACM* **2013**, *56*, 94–103. [CrossRef]

10. Ding, W.; Hu, H. On the safety of iot device physical interaction control. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 15–19 October 2018; pp. 832–846.

11. Jin, Z.; Xing, L.; Fang, Y.; Jia, Y.; Yuan, B.; Liu, Q. P-Verifier: Understanding and Mitigating Security Risks in Cloud-based IoT Access Policies. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 7–11 November 2022; pp. 1647–1661.

12. Samad, A.; Alam, S.; Mohammed, S.; Bhukhari, M. Internet of vehicles (IoV) requirements, attacks and countermeasures. In Proceedings of the 12th INDIACom; INDIACom-2018; 5th International Conference on "Computing for Sustainable Global Development" IEEE Conference, New Delhi, India, 14–16 March 2018; pp. 1–4.

13. Michelena, A.; Aveleira-Mata, J.; Jove, E.; Bayón-Gutiérrez, M.; Novais, P.; Romero, O.F.; Calvo-Rolle, J.L.; Aláiz-Moretón, H. A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. *Expert Syst.* **2024**, *41*, e13263. [CrossRef]

14. Sivasankari, N.; Kamalakkannan, S. Detection and prevention of man-in-the-middle attack in iot network using regression modeling. *Adv. Eng. Softw.* **2022**, *169*, 103126. [CrossRef]

15. Chaudhary, S.; Mishra, P.K. DDoS attacks in Industrial IoT: A survey. *Comput. Netw.* **2023**, *236*, 110015. [CrossRef]

16. Yang, W.; Wang, S.; Yin, X.; Wang, X.; Hu, J. A review on security issues and solutions of the Internet of Drones. *IEEE Open J. Comput. Soc.* **2022**, *3*, 96–110. [CrossRef]

17. Surya, L. Security challenges and strategies for the IoT in cloud computing. *Int. J. Innov. Eng. Res. Technol. ISSN* **2016**, *3*, 2394–3696.

18. Georgakopoulos, D.; Jayaraman, P.P.; Fazia, M.; Villari, M.; Ranjan, R. Internet of Things and edge cloud computing roadmap for manufacturing. *IEEE Cloud Comput.* **2016**, *3*, 66–73. [CrossRef]

19. Zhou, J.; Leppanen, T.; Harjula, E.; Ylianttila, M.; Ojala, T.; Yu, C.; Jin, H.; Yang, L.T. Cloudthings: A common architecture for integrating the internet of things with cloud computing. In Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Whistler, BC, Canada, 27–29 June 2013; pp. 651–657.

20. Shafique, K.; Khawaja, B.A.; Sabir, F.; Qazi, S.; Mustaqim, M. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access* **2020**, *8*, 23022–23040. [CrossRef]

21. Atlam, H.F.; Alenezi, A.; Alharthi, A.; Walters, R.J.; Wills, G.B. Integration of cloud computing with internet of things: Challenges and open issues. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 670–675.

22. Cai, H.; Xu, B.; Jiang, L.; Vasilakos, A.V. IoT-based big data storage systems in cloud computing: Perspectives and challenges. *IEEE Internet Things J.* **2016**, *4*, 75–87. [CrossRef]

23. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access* **2021**, *9*, 28177–28193. [CrossRef]

24. Chen, F.; Luo, D.; Xiang, T.; Chen, P.; Fan, J.; Truong, H.L. IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-Oriented Applications. *ACM Comput. Surv.* **2021**, *54*. [CrossRef]

25. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *D* **2017**, *88*, 10–28. [CrossRef]

26. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A. A review of security in internet of things. *Wirel. Pers. Commun.* **2019**, *108*, 325–344. [CrossRef]

27. Yousefnezhad, N.; Malhi, A.; Främling, K. Security in product lifecycle of IoT devices: A survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102779. [CrossRef]

28. Almolhis, N.; Alashjaee, A.M.; Duraibi, S.; Alqahtani, F.; Moussa, A.N. The security issues in IoT-cloud: A review. In Proceedings of the 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 28–29 February 2020; pp. 191–196.

29. Lit, Y.; Kim, S.; Sy, E. A survey on amazon alexa attack surfaces. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–7.

30. Ling, L.; Yelland, N.; Hatzigianni, M.; Dickson-Deane, C. The use of Internet of Things devices in early childhood education: A systematic review. *Educ. Inf. Technol.* **2022**, *27*, 6333–6352. [CrossRef]

31. Shah, K.; Sheth, C.; Doshi, N. A survey on iot-based smart cars, their functionalities and challenges. *Procedia Comput. Sci.* **2022**, *210*, 295–300. [CrossRef]

32. Sicari, S.; Rizzardi, A.; Coen-Porisini, A. How to evaluate an Internet of Things system: Models, case studies, and real developments. *Softw. Pract. Exp.* **2019**, *49*, 1663–1685. [CrossRef]

33. Sivaraman, V.; Chan, D.; Earl, D.; Boreli, R. Smart-phones attacking smart-homes. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 18–2 July 2016; pp. 195–200.

34. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1191–1221. [CrossRef]

35. Domingo-Ferrer, J.; Farras, O.; Ribes-González, J.; Sánchez, D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Comput. Commun.* **2019**, *140*, 38–60. [CrossRef]

36. Ahmed, N.; Khan, J.; Sheta, N.; Tarek, R.; Zualkernan, I.; Aloul, F. Detecting Replay Attack on Voice-Controlled Systems using Small Neural Networks. In Proceedings of the 2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI), Paris, France, 24–26 August 2022; pp. 50–54.

37. Obaid, A.J. Assessment of smart home assistants as an IoT. *Int. J. Comput. Inf. Manuf. (IJCIM)* **2021**, *1*. [CrossRef]

38. Zhang, N.; Mi, X.; Feng, X.; Wang, X.; Tian, Y.; Qian, F. Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1381–1396.

39. Kumar, D.; Paccagnella, R.; Murley, P.; Hennenfent, E.; Mason, J.; Bates, A.; Bailey, M. Skill squatting attacks on Amazon Alexa. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 33–47.

40. Wollerton, M. Samsung SmartThings Still Hasn't Earned My Trust in the Smart Home. *CNET* **2024**. Available online: https://www.cnet.com/home/smart-home/samsung-smartthings-still-hasnt-earned-my-trust-in-the-smart-home/ (accessed on 6 June 2024).

41. Fernandes, E.; Jung, J.; Prakash, A. Security analysis of emerging smart home applications. In Proceedings of the 2016 IEEE symposium on security and privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 636–654.

42. Fernandes, E.; Rahmati, A.; Jung, J.; Prakash, A. Security implications of permission models in smart-home application frameworks. *IEEE Secur. Priv.* **2017**, *15*, 24–30. [CrossRef]

43. Zhang, W.; Meng, Y.; Liu, Y.; Zhang, X.; Zhang, Y.; Zhu, H. Homonit: Monitoring smart home apps from encrypted traffic. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1074–1088.

44. Otoom, A.F.; Eleisah, W.; Abdallah, E.E. Deep learning for accurate detection of brute force attacks on IOT Networks. *Procedia Comput. Sci.* **2023**, *220*, 291–298. [CrossRef]

45. Attoh, E.; Signer, B. Towards a Write Once Run Anywhere Approach in End-User IoT Development. In Proceedings of the 9th International Conference on Internet of Things, Bilbao, Spain, 22–25 October 2024.

46. Sanlı, M. Detection and Mitigation of Denial of Service Attacks in Internet of Things Networks. *Arab. J. Sci. Eng.* **2024**, *49*, 12629–12639. [CrossRef]

47. Cloudflare. Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis. 2024. Available online: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ (accessed on 13 May 2024).

48. Aziz Al Kabir, M.; Elmedany, W.; Sharif, M.S. Securing IoT devices against emerging security threats: Challenges and mitigation techniques. *J. Cyber Secur. Technol.* **2023**, *7*, 199–223. [CrossRef]

49. Navas, R.E.; Le Bouder, H.; Cuppens, N.; Cuppens, F.; Papadopoulos, G.Z. Do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack. In Proceedings of the Ad-Hoc, Mobile, and Wireless Networks: 17th International Conference on Ad Hoc Networks and Wireless, ADHOC-NOW 2018, Saint-Malo, France, 5–7 September 2018; Springer: Cham, Switzerland, 2018; pp. 120–125.

50. Sharma, A.; Dyrkolbotn, G.O.; Øverlier, L.; Waltoft-Olsen, A.J.; Franke, K.; Katsikas, S. A state-of-the-art reverse engineering approach for combating hardware security vulnerabilities at the system and pcb level in iot devices. In Proceedings of the 2022 IEEE Physical Assurance and Inspection of Electronics (PAINE), Huntsville, AL, USA, 25–27 October 2022; pp. 1–7.

51. Park, M.; Oh, H.; Lee, K. Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors* **2019**, *19*, 2148. [CrossRef]

52. Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.K.R. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 17–25. [CrossRef]

53. Obermaier, J.; Hutle, M. Analyzing the security and privacy of cloud-based video surveillance systems. In Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, Xi'an, China, 30 May 2016; pp. 22–28.

54. Seralathan, Y.; Oh, T.T.; Jadhav, S.; Myers, J.; Jeong, J.P.; Kim, Y.H.; Kim, J.N. IoT security vulnerability: A case study of a Web camera. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, South Korea, 11–14 February 2018; pp. 172–177.

55. Tekeoglu, A.; Tosun, A.S. Investigating security and privacy of a cloud-based wireless IP camera: NetCam. In Proceedings of the 2015 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas, NV, USA, 3–6 August 2015; pp. 1–6.

56. Xu, H.; Xu, F.; Chen, B. Internet protocol cameras with no password protection: An empirical investigation. In Proceedings of the International Conference on Passive and Active Network Measurement, Berlin, Germany, 26–27 March 2018; Springer: Cham, Switzerland, 2018; pp. 47–59.

57. Mangala, N.; Venugopal, K.; Eswara Reddy, B. Current Challenges in IoT Cloud Smart Applications. In Proceedings of the 2021 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), New Jersey, USA, 27–30 October 2021; pp. 36–40.

58. Geeng, C.; Roesner, F. Who's in control? Interactions in multi-user smart homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Scotland, UK, 4–9 May 2019; pp. 1–13.

59. Jang, W.; Chhabra, A.; Prasad, A. Enabling multi-user controls in smart home devices. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Glasgow, UK, 4–9 May 2017; pp. 49–54.

60. Zeng, E.; Roesner, F. Understanding and Improving Security and Privacy in {Multi-User} Smart Homes: A Design Exploration and {In-Home} User Study. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 159–176.

61. Davis, B.D.; Mason, J.C.; Anwar, M. Vulnerability studies and security postures of IoT devices: A smart home case study. *IEEE Internet Things J.* **2020**, *7*, 10102–10110. [CrossRef]

62. Notra, S.; Siddiqi, M.; Gharakheili, H.H.; Sivaraman, V.; Boreli, R. An experimental study of security and privacy risks with emerging household appliances. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 79–84.

63. Ren, Y.; Peng, H.; Li, L.; Xue, X.; Lan, Y.; Yang, Y. A voice spoofing detection framework for IoT systems with feature pyramid and online knowledge distillation. *J. Syst. Archit.* **2023**, *143*, 102981. [CrossRef]

64. Hooda, A.; Wallace, M.; Jhunjhunwalla, K.; Fernandes, E.; Fawaz, K. SkillFence: A Systems Approach to Practically Mitigating Voice-Based Confusion Attacks. *Proc. Acm Interact. Mob. Wearable Ubiquitous Technol.* **2022**, *6*, 1–26. [CrossRef]

65. Chatterjee, U.; Chakraborty, R.S.; Mukhopadhyay, D. A PUF-based secure communication protocol for IoT. *ACM Trans. Embed. Comput. Syst. (TECS)* **2017**, *16*, 1–25. [CrossRef]

66. Nazzal, B.; Zaid, A.A.; Alalfi, M.H.; Valani, A. Vulnerability classification of consumer-based IoT software. In Proceedings of the 4th International Workshop on Software Engineering Research and Practice for the IoT, Pittsburgh, PA, USA, 19 May 2022; pp. 17–24.

67. Shameli-Sendi, A.; Pourzandi, M.; Fekih-Ahmed, M.; Cheriet, M. Taxonomy of distributed denial of service mitigation approaches for cloud computing. *J. Netw. Comput. Appl.* **2015**, *58*, 165–179. [CrossRef]

68. Salva-Garcia, P.; Alcaraz-Calero, J.M.; Wang, Q.; Bernabe, J.B.; Skarmeta, A. 5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks. *Secur. Commun. Netw.* **2018**, *2018*, 1–21. [CrossRef]

69. Guozi, S.; Jiang, W.; Yu, G.; Danni, R.; Huakang, L. DDoS attacks and flash event detection based on flow characteristics in SDN. In Proceedings of the 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 27–30 November 2018; pp. 1–6.

70. Yan, Q.; Huang, W.; Luo, X.; Gong, Q.; Yu, F.R. A multi-level DDoS mitigation framework for the industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 30–36. [CrossRef]

71. Ma, D.; Xu, Z.; Lin, D. Defending blind DDoS attack on SDN based on moving target defense. In Proceedings of the International Conference on Security and Privacy in Communication Networks: 10th International ICST Conference, SecureComm 2014, Beijing, China, 24–26 September 2014; Springer: Cham, Swizterland, 2015; pp. 463–480.

72. Connell, W.; Menascé, D.A.; Albanese, M. Performance modeling of moving target defenses. In Proceedings of the 2017 Workshop on Moving Target Defense, Dallas, TX, USA, 30 October 2017; pp. 53–63.

73. Chen, W.; Xiao, S.; Liu, L.; Jiang, X.; Tang, Z. A DDoS attacks traceback scheme for SDN-based smart city. *Comput. Electr. Eng.* **2020**, *81*, 106503. [CrossRef]

74. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. Secure IoT structural design for smart homes. In *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 187–201.

75. Abu-Tair, M.; Djahel, S.; Perry, P.; Scotney, B.; Zia, U.; Carracedo, J.M.; Sajjad, A. Towards secure and privacy-preserving IoT enabled smart home: architecture and experimental study. *Sensors* **2020**, *20*, 6131. [CrossRef]

76. Qasem, M.A.; Thabit, F.; Can, O.; Naji, E.; Alkhzaimi, H.A.; Patil, P.R.; Thorat, S. Cryptography algorithms for improving the security of cloud-based internet of things. *Secur. Priv.* **2024**, *7*, e378. [CrossRef]

77. Gerber, P.; Heidinger, M.; Stiegelmayer, J.; Gerber, N. LOKI: Development of an interface for task-based, privacy-friendly smart home control through LOCal Information Processing: LOKI: Entwicklung eines Interfaces für die Aufgaben-basierte, Privatsphäre-freundliche Smart Home-Steuerung durch LOKale Informationsverarbeitung. In Proceedings of the Mensch und Computer 2021, Ingolstadt, Germany, 5–8 September 2021; pp. 578–581.

78. Child Protection Services. Children's Online Privacy Protection Rule ("COPPA"). Federal Trade Commission. 2023. Available online: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (accessed on 17 July 2023).

79. Holloway, D.; Green, L. The internet of toys. *Commun. Res. Pract.* **2016**, *2*, 506–519. [CrossRef]

80. Ataei Nezhad, M.; Barati, H.; Barati, A. An authentication-based secure data aggregation method in Internet of Things. *J. Grid Comput.* **2022**, *20*, 29. [CrossRef] [PubMed]

81. Hung, P.C.; Iqbal, F.; Huang, S.C.; Melaisi, M.; Pang, K. A glance of child's play privacy in smart toys. In Proceedings of the International Conference on Cloud Computing and Security, Nanjing, China, 29–31 July 2016; Springer: Cham, Switzerland, 2016; pp. 217–231.

82. Valente, J.; Cardenas, A.A. Security & privacy in smart toys. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, TX, USA, 3 November 2017; pp. 19–24.

83. Albrecht, K.; Mcintyre, L. Privacy nightmare: When baby monitors go bad [opinion]. *IEEE Technol. Soc. Mag.* **2015**, *34*, 14–19. [CrossRef]

84. Stanislav, M.; Beardsley, T. *Hacking Iot: A Case Study on Baby Monitor Exposures and Vulnerabilities*; Rapid7 Report; Rapid7: Boston, MA, USA, 2015.

85. Rivera, D.; García, A.; Martín-Ruiz, M.L.; Alarcos, B.; Velasco, J.R.; Oliva, A.G. Secure communications and protected data for a Internet of Things smart toy platform. *IEEE Internet Things J.* **2019**, *6*, 3785–3795. [CrossRef]

86. Rafferty, L.; Hung, P.C.; Fantinato, M.; Peres, S.M.; Iqbal, F.; Kuo, S.Y.; Huang, S.C. Towards a privacy rule conceptual model for smart toys. In *Computing in Smart Toys*; Springer: Cham, Switzerland, 2017; pp. 85–102.

87. Yankson, B.; Iqbal, F.; Hung, P.C. 4P-based forensics investigation framework for smart connected toys. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual, 25–28 August 2020; pp. 1–9.

88. Thales. IoT in Healthcare. Thales Group. 2022. Available online: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/industries/healthcare (accessed on 13 May 2024).

89. Ganesh, K.V.S.S.; Jeyanth, S.S.; Bevi, A.R. IOT based portable heart rate and SpO2 pulse oximeter. *HardwareX* **2022**, *11*, e00309. [CrossRef]

90. Okafor, S.A.; Arukalam, F.M.; Ekuma, I.C.; Eziefuna, E.O.; Ihetu, C.A.; Okey-Mbata, C.C.; Ezeamaku, U.L.; Iheaturu, N.C.; Okafor, A.L. Design and Development of an Internet of things Based Glucometer with Wireless Transmission. *J. Eng. Res. Rep.* **2022**, *22*, 36–46. [CrossRef]

91. Intellectsoft. Biggest IoT Security Issues. *Intellectsoft* **2024**. Available online: https://www.intellectsoft.net/blog/biggest-iot-security-issues/ (accessed on 11 May 2024).

92. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Gener. Comput. Syst.* **2018**, *78*, 659–676. [CrossRef]

93. McAllister, T.D.; El-Tawab, S.; Heydari, M.H. Localization of health center assets through an iot environment (locate). In Proceedings of the 2017 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 28 April 2017; pp. 132–137.

94. Flynn, T.; Grispos, G.; Glisson, W.; Mahoney, W. Knock! knock! Who is there? Investigating data leakage from a medical internet of things hijacking attack. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2020.

95. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]

96. West, J.; Kohno, T.; Lindsay, D.; Sechman, J. Wearfit: Security design analysis of a wearable fitness tracker. In *IEEE Center for Secure Design*; IEEE: New York, NY, USA, 2016.

97. Food, U.; Administration, D. Postmarket Management of Cybersecurity in Medical Devices. *US Food and Drug Administration* **2023**. Available online: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices (accessed on 9 May 2023).

98. Wazid, M.; Bera, B.; Mitra, A.; Das, A.K.; Ali, R. Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 37–42.

99. Fathalizadeh, A.; Moghtadaiee, V.; Alishahi, M. On the privacy protection of indoor location dataset using anonymization. *Comput. Secur.* **2022**, *117*, 102665. [CrossRef]

100. Arul, R.; Alroobaea, R.; Tariq, U.; Almulihi, A.H.; Alharithi, F.S.; Shoaib, U. IoT-enabled healthcare systems using block chain-dependent adaptable services. *Pers. Ubiquitous Comput.* **2024**, *28*, 43–57. [CrossRef]

101. Bu, L.; Karpovsky, M.G.; Kinsy, M.A. Bulwark: Securing implantable medical devices communication channels. *Comput. Secur.* **2019**, *86*, 498–511. [CrossRef]

102. Ma, Y.; Ma, R.; Lin, Z.; Zhang, R.; Cai, Y.; Wu, W.; Wang, J. Improving age of information for covert communication with time-modulated arrays. *IEEE Internet Things J.* **2024**. [CrossRef]

103. Saeedi, K. Machine Learning for DDOS Detection in Packet Core Network for IoT. Master's Thesis, Luleå University of Technology, Luleå, Sweden, 2019.

104. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. Healthguard: A machine learning-based security framework for smart healthcare systems. In Proceedings of the 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), Granada, Spain, 22–25 October 2019; pp. 389–396.

105. Srivastava, G.; Crichigno, J.; Dhar, S. A light and secure healthcare blockchain for iot medical devices. In Proceedings of the 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–5.

106. Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. Data sharing and privacy for patient iot devices using blockchain. In Proceedings of the Smart City and Informatization: 7th International Conference, iSCI 2019, Guangzhou, China, 12–15 November 2019; Springer: Cham, Switzerland, 2019; pp. 334–348.

107. Shrivastava, R.K.; Singh, S.P.; Hasan, M.K.; Islam, S.; Abdullah, S.; Aman, A.H.M.; Mohd Aman, A.H. Securing Internet of Things devices against code tampering attacks using Return Oriented Programming. *Comput. Commun.* **2022**, *193*, 38–46. [CrossRef]

108. Wu, T.F.; Ganesan, K.; Hu, Y.A.; Wong, H.S.P.; Wong, S.; Mitra, S. TPAD: Hardware Trojan prevention and detection for trusted integrated circuits. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2015**, *35*, 521–534. [CrossRef]

109. Rathore, H.; Mohamed, A.; Guizani, M. Deep learning-based security schemes for implantable medical devices. In *Energy Efficiency of Medical Devices and Healthcare Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 109–130.

110. Li, J.; Cai, J.; Khan, F.; Rehman, A.U.; Balasubramaniam, V.; Sun, J.; Venu, P. A secured framework for sdn-based edge computing in IOT-enabled healthcare system. *IEEE Access* **2020**, *8*, 135479–135490. [CrossRef]

111. Zverev, M.; Agüero, R.; Garrido, P.; Bilbao, J. Network Coding for IIoT Multi-Cloud Environments. In Proceedings of the 9th International Conference on the Internet of Things, Bilbao, Spain, 22–25 October 2019; pp. 1–4.

112. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.

113. Anderson, R.J.; Fuloria, S. *Smart Meter Security: A Survey*; University of Cambridge: Cambridge, UK, 2011.

114. Cleemput, S.; Mustafa, M.A.; Preneel, B. High assurance smart metering. In Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE), Orlando, FL, USA, 7–9 January 2016; pp. 294–297.

115. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.R.; Jin, Y. Security analysis on consumer and industrial IoT devices. In Proceedings of the 2016 21st Asia and South Pacific design automation conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 519–524.

116. Horak, T.; Strelec, P.; Huraj, L.; Tanuska, P.; Vaclavova, A.; Kebisek, M. The vulnerability of the production line using industrial IoT systems under ddos attack. *Electronics* **2021**, *10*, 381. [CrossRef]

117. Soltan, S.; Mittal, P.; Poor, H.V. {BlackIoT}:{IoT} botnet of high wattage devices can disrupt the power grid. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 15–32.

118. Tu, Y.; Rampazzi, S.; Hao, B.; Rodriguez, A.; Fu, K.; Hei, X. Trick or heat? Manipulating critical temperature-based control systems using rectification attacks. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2301–2315.

119. Ahamad, R.; Mishra, K.N. Hybrid approach for suspicious object surveillance using video clips and UAV images in cloud-IoT-based computing environment. *Clust. Comput.* **2024**, *27*, 761–785. [CrossRef]

120. Kott, A.; Swami, A.; West, B.J. The internet of battle things. *Computer* **2016**, *49*, 70–75. [CrossRef]

121. Lesjak, C.; Bock, H.; Hein, D.; Maritsch, M. Hardware-secured and transparent multi-stakeholder data exchange for industrial IoT. In Proceedings of the 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), Poitiers, France, 19–21 July 2016; pp. 706–713.

122. Pu, L.; Lin, C.; Chen, B.; He, D. User-friendly public-key authenticated encryption with keyword search for industrial internet of things. *IEEE Internet Things J.* **2023**, *10*, 13544–13555. [CrossRef]

123. Tan, L.; Yu, K.; Yang, C.; Bashir, A.K. A blockchain-based Shamir's threshold cryptography for data protection in industrial internet of things of smart city. In Proceedings of the 1st Workshop on Artificial Intelligence and Blockchain Technologies for Smart Cities with 6G, New Orleans, LA, USA, 25–29 October 2021; pp. 13–18.

124. De Oliveira, G.W.; Nogueira, M.; dos Santos, A.L.; Batista, D.M. Intelligent VNF placement to mitigate DDoS attacks on industrial IoT. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 1319–1331. [CrossRef]

125. Ibrahim, R.F.; Abu Al-Haija, Q.; Ahmad, A. DDoS attack prevention for internet of thing devices using ethereum blockchain technology. *Sensors* **2022**, *22*, 6806. [CrossRef] [PubMed]

126. Li, J.; Lyu, L.; Liu, X.; Zhang, X.; Lyu, X. FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4059–4068. [CrossRef]

127. Kuusijärvi, J.; Savola, R.; Savolainen, P.; Evesti, A. Mitigating IoT security threats with a trusted Network element. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016; pp. 260–265.

128. Stocchero, J.M.; Silva, C.A.; de Souza Silva, L.; Lawisch, M.A.; dos Anjos, J.C.S.; de Freitas, E.P. Secure command and control for internet of battle things using novel network paradigms. *IEEE Commun. Mag.* **2022**, *61*, 166–172. [CrossRef]

129. Tbatou, S.; Ramrami, A.; Tabii, Y. Security of communications in connected cars modeling and safety assessment. In Proceedings of the 2nd International Conference on Big Data, Cloud and Applications, Tetouan, Morocco, 29–30 March 2017; pp. 1–7.

130. Zhu, Y.; Zeng, J.; Weng, F.; Han, D.; Yang, Y.; Li, X.; Zhang, Y. Sybil attacks detection and traceability mechanism based on beacon packets in connected automobile vehicles. *Sensors* **2024**, *24*, 2153. [CrossRef] [PubMed]

131. Kumar, R.; Sharma, R.; Pattnaik, P.K. *Multimedia Technologies in the Internet of Things Environment*; Springer: Singapore, 2021; Volume 2.

132. Taslimasa, H.; Dadkhah, S.; Neto, E.C.P.; Xiong, P.; Ray, S.; Ghorbani, A.A. Security issues in Internet of Vehicles (IoV): A comprehensive survey. *Internet Things* **2023**, *22*, 100809. [CrossRef]

133. Zhang, R.; Cheng, L.; Wang, S.; Lou, Y.; Gao, Y.; Wu, W.; Ng, D.W.K. Integrated sensing and communication with massive MIMO: A unified tensor approach for channel and target parameter estimation. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 8571–8587. [CrossRef]

134. Khan, S.K.; Shiwakoti, N.; Stasinopoulos, P.; Chen, Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accid. Anal. Prev.* **2020**, *148*, 105837. [CrossRef]

135. Zewdie, T.G.; Girma, A. IOT Security and the Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment. *Issues Inf. Syst.* **2020**, *21*, 253–263.

136. Smys, S.; Wang, H. Security enhancement in smart vehicle using blockchain-based architectural framework. *J. Artif. Intell.* **2021**, *3*, 90–100.

137. Zhao, C.; Gill, J.S.; Pisu, P.; Comert, G. Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 9078–9088. [CrossRef]

138. Balas, V.E.; Solanki, V.K.; Kumar, R.; Ahad, M.A.R. *A Handbook of Internet of Things in Biomedical and Cyber Physical System*; Technical Report; Springer: Cham, Switzerland, 2020.

139. Lee, L.; Egelman, S.; Lee, J.H.; Wagner, D. Risk perceptions for wearable devices. *arXiv* **2015**, arXiv:1504.05694.

140. Siboni, S.; Shabtai, A.; Tippenhauer, N.O.; Lee, J.; Elovici, Y. Advanced security testbed framework for wearable IoT devices. *ACM Trans. Internet Technol. (TOIT)* **2016**, *16*, 1–25. [CrossRef]

141. Lennon, M. All smartwatches vulnerable to attack: HP study. *Retrieved Novemb.* **2015**, *28*, 2015.

142. Cusack, B.; Antony, B.; Ward, G.; Mody, S. Assessment of security vulnerabilities in wearable devices. In Proceedings of the 15th Australian Information Security Management Conference, Perth, Australia, 5–6 December 2017.

143. Giaretta, A. Security and Privacy in Virtual Reality–A Literature Survey. *arXiv* **2022**, arXiv:2205.00208. [CrossRef]

144. Adams, D.; Bah, A.; Barwulor, C.; Musaby, N.; Pitkin, K.; Redmiles, E.M. Ethics emerging: The story of privacy and security perceptions in virtual reality. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Berkeley, CA, USA, 12–14 August 2018; pp. 427–442.

145. Karakaya, M.; Bostan, A.; Gökçay, E. How Secure is Your Smart Watch? *Int. J. Inf. Secur. Sci.* **2016**, *5*, 90–95.

146. Mahinderjit Singh, M.; Ching, K.W.; Abd Manaf, A. A novel out-of-band biometrics authentication scheme for wearable devices. *Int. J. Comput. Appl.* **2020**, *42*, 589–601. [CrossRef]

147. Kavianpour, S.; Shanmugam, B.; H Zolait, A.; Razaq, A. A Framework to Detect Cyber-attacks against Networked Medical Devices (Internet of Medical Things): An Attack-Surface-Reduction by Design Approach. *Int. J. Comput. Digit. Syst.* **2021**, *11*, 1289–1298.

148. Bhatia, M.; Sangwan, S.R. Soft computing for anomaly detection and prediction to mitigate IoT-based real-time abuse. *Pers. Ubiquitous Comput.* **2021**, *28*, 123–133. [CrossRef]

149. Zhao, T.; Wang, Y.; Liu, J.; Chen, Y.; Cheng, J.; Yu, J. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020; pp. 30–39.

150. Gulhane, A.; Vyas, A.; Mitra, R.; Oruche, R.; Hoefer, G.; Valluripally, S.; Calyam, P.; Hoque, K.A. Security, privacy and safety risk assessment for virtual reality learning environment applications. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–9.

151. Fang, L.; Li, M.; Zhou, L.; Zhang, H.; Ge, C. A fine-grained user-divided privacy-preserving access control protocol in smart watch. *Sensors* **2019**, *19*, 2109. [CrossRef]

152. IoT Now. Analyst Insights on IoT in the Retail Sector. 2022. Available online: https://www.iot-now.com/2022/07/18/122379-insights-on-retail-sector/ (accessed on 21 April 2024).

153. Wang, B.; Xie, Y.; Duan, X. An IoT Based Fruit and Vegetable Sales System: A whole system including IoT based integrated intelligent scale and online shop. In Proceedings of the 2021 5th International Conference on Cloud and Big Data Computing, Liverpool, UK, 13–15 August 2021; pp. 109–115.

154. Di Rienzo, A.; Garzotto, F.; Cremonesi, P.; Frà, C.; Valla, M. Towards a smart retail environment. In Proceedings of the Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers, Osaka, Japan, 1–7 September 2015; pp. 779–782.

155. Nozomi Networks. IoT Cybersecurity for Retail Organizations. 2024. Available online: https://www.nozominetworks.com/industries/retail-cybersecurity (accessed on 21 May 2024).

156. Mitzner, D. IoT And The Rise Of Cyber Security Threats In Retail. *Forbes* **2022**. Available online: https://www.forbes.com/sites/dennismitzner/2022/09/14/self-checkouts-iot-and-the-rise-of-retail-cyber-security-threats/?sh=683e47b157f5 (accessed on 5 November 2024).

157. Singh, N.; Do, Y.; Fouad, Y.Y.I.; Kim, J.; Kim, H. Crumbled Cookie Exploring E-commerce Websites Cookie Policies with Data Protection Regulations. *ACM TWEB* **2024**. [CrossRef]

158. Mavroudis, V.; Veale, M. Eavesdropping whilst you're shopping: Balancing personalisation and privacy in connected retail spaces. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018; pp. 1–10.

159. Cartwright, A.; Cartwright, E. The economics of ransomware attacks on integrated supply chain networks. *Digit. Threat. Res. Pract.* **2023**, *4*, 56. [CrossRef]

160. Wang, S.; Tu, G.H.; Lei, X.; Xie, T.; Li, C.Y.; Chou, P.Y.; Hsieh, F.; Hu, Y.; Xiao, L.; Peng, C. Insecurity of operational cellular IoT service: New vulnerabilities, attacks, and countermeasures. In Proceedings of the 27th Annual International Conference on Mobile Computing and Networking, New Orleans, LA, USA, 25–29 October 2021; pp. 437–450.

161. Jaffar, J.A.; Elmedany, W. A systematic review of homomorphic encryption applications in Internet of Things. In Proceedings of the 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain, 6–8 December 2022; Volume 2022, pp. 489–497.

162. Musa, Z.; Vidyasankar, K. A fog computing framework for blackberry supply chain management. *Procedia Comput. Sci.* **2017**, *113*, 178–185. [CrossRef]

163. Brasilino, L.R.; Swany, M. Mitigating ddos flooding attacks against iot using custom hardware modules. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 58–64.

164. Das, S. An IoT business model for public sector retail oil outlets. *Inf. Technol. People* **2022**, *35*, 2344–2367. [CrossRef]

165. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]

166. Akhter, R.; Sofi, S.A. Precision agriculture using IoT data analytics and machine learning. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5602–5618. [CrossRef]

167. Singh, N.; Singh, A.N. Odysseys of agriculture sensors: Current challenges and forthcoming prospects. *Comput. Electron. Agric.* **2020**, *171*, 105328. [CrossRef]

168. Namani, S.; Gonen, B. Smart agriculture based on IoT and cloud computing. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; pp. 553–556.

169. Patil, V.; Al-Gaadi, K.; Biradar, D.; Rangaswamy, M. Internet of things (Iot) and cloud computing for agriculture: An overview. In Proceedings of Agro-Informatics and Precision Agriculture (AIPA 2012), Hyderabad, India, 1–3 August 2012; pp. 292–296.

170. Mekala, M.S.; Viswanathan, P. A Survey: Smart agriculture IoT with cloud computing. In Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–7.

171. Krzywoszynska, A. Soil care: Understanding soil needs, responsibilities, and attentiveness through the concept of care. *Preprint*. Available online: https://www.researchgate.net/publication/349368854_Soil_care_understanding_soil_needs_responsibilities_and_attentiveness_through_the_concept_of_care?channel=doi&linkId=602d07ae4585158939adc1f5&showFulltext=true (accessed on 13 May 2023).

172. Yu, L.; Gao, W.; R Shamshiri, R.; Tao, S.; Ren, Y.; Zhang, Y.; Su, G. Review of research progress on soil moisture sensor technology. *Int. J. Agric. Biol. Eng.* **2021**, *14*, 32–42. [CrossRef]

173. Refaai, M.R.; Dattu, V.S.; Gireesh, N.; Dixit, E.; Sandeep, C.; Christopher, D. Application of IoT-Based Drones in Precision Agriculture for Pest Control. *Adv. Mater. Sci. Eng.* **2022**, *2022*, 1160258. [CrossRef]

174. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]

175. Song, C.; Ma, W.; Li, J.; Qi, B.; Liu, B. Development Trends in Precision Agriculture and Its Management in China Based on Data Visualization. *Agronomy* **2022**, *12*, 2905. [CrossRef]

176. Salam, A.; Salam, A. Internet of things for sustainability: Perspectives in privacy, cybersecurity, and future trends. In *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*; Springer: Cham, Switzerland, 2020; pp. 299–327.

177. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]

178. Mori, H.; Kundaliya, J.; Naik, K.; Shah, M. IoT technologies in smart environment: Security issues and future enhancements. *Environ. Sci. Pollut. Res.* **2022**, *29*, 47969–47987. [CrossRef] [PubMed]

179. Triantafyllou, A.; Sarigiannidis, P.; Bibi, S. Precision agriculture: A remote sensing monitoring system architecture. *Information* **2019**, *10*, 348. [CrossRef]

180. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]

181. Glaroudis, D.; Iossifides, A.; Chatzimisios, P. Survey, comparison and research challenges of IoT application protocols for smart farming. *Comput. Netw.* **2020**, *168*, 107037. [CrossRef]

182. Farooq, M.S.; Riaz, S.; Abid, A.; Abid, K.; Naeem, M.A. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access* **2019**, *7*, 156237–156271. [CrossRef]

183. Madushanki, A.R.; Halgamuge, M.N.; Wirasagoda, W.S.; Ali, S. Adoption of the Internet of Things (IoT) in agriculture and smart farming towards urban greening: A review. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 11–28. [CrossRef]

184. Ahmed, N.; De, D.; Hussain, I. Internet of Things (IoT) for smart precision agriculture and farming in rural areas. *IEEE Internet Things J.* **2018**, *5*, 4890–4899. [CrossRef]

185. Raghuvanshi, A.; Singh, U.K.; Sajja, G.S.; Pallathadka, H.; Asenso, E.; Kamal, M.; Singh, A.; Phasinam, K. Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming. *J. Food Qual.* **2022**, *2022*, 1–8. [CrossRef]

186. Kondaveeti, H.K.; Sai, G.B.; Athar, S.A.; Vatsavayi, V.K.; Mitra, A.; Ananthachari, P. Federated Learning for Smart Agriculture: Challenges and Opportunities. In Proceedings of the 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 26–27 April 2024; pp. 1–7.

187. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Gadekallu, T.R.; Srivastava, G. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. *Comput. Netw.* **2021**, *187*, 107819. [CrossRef]

188. Kethineni, K.; Gera, P. IoT-based privacy-preserving anomaly detection model for smart agriculture. *Systems* **2023**, *11*, 304. [CrossRef]

189. Song, J.; Zhong, Q.; Wang, W.; Su, C.; Tan, Z.; Liu, Y. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. *IEEE Sens. J.* **2020**, *21*, 17430–17438. [CrossRef]

190. Zhou, M.; Zheng, Y.; Guan, Y.; Peng, L.; Lu, R. Efficient and privacy-preserving range-max query in fog-based agricultural IoT. *Peer-Peer Netw. Appl.* **2021**, *14*, 2156–2170. [CrossRef]

191. Chukkapalli, S.S.L.; Ranade, P.; Mittal, S.; Joshi, A. A Privacy-Preserving Anomaly Detection Framework for Cooperative Smart Farming Ecosystem. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 340–347.

192. Kumar, P.; Gupta, G.P.; Tripathi, R. PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture. *IEEE Micro* **2021**, *42*, 33–40. [CrossRef]

193. Malik, J.A.; Hussain, A.; Shah, H.; Saleem, M.; alsanoosy, T.; Chaudhary, U.M.D. Optimizing Agricultural Risk Management with Hybrid Block-Chain and Fog Computing Architectures for Secure and Efficient Data Handling. In *Computational Intelligence in Internet of Agricultural Things*; Springer: Cham, Switzerland, 2024; pp. 309–337.

194. Anidu, A.; Dara, R. A review of data governance challenges in smart farming and potential solutions. In Proceedings of the 2021 IEEE International Symposium on Technology and Society (ISTAS), Waterloo, ON, Canada, 28–31 October 2021; pp. 1–8.

195. Chaganti, R.; Varadarajan, V.; Gorantla, V.S.; Gadekallu, T.R.; Ravi, V. Blockchain-based cloud-enabled security monitoring using Internet of Things in smart agriculture. *Future Internet* **2022**, *14*, 250. [CrossRef]

196. Al-Turjman, F.; Abujubbeh, M. IoT-enabled smart grid via SM: An overview. *Future Gener. Comput. Syst.* **2019**, *96*, 579–590. [CrossRef]

197. Pau, M.; Patti, E.; Barbierato, L.; Estebsari, A.; Pons, E.; Ponci, F.; Monti, A. A cloud-based smart metering infrastructure for distribution grid services and automation. *Sustain. Energy, Grids Netw.* **2018**, *15*, 14–25. [CrossRef]

198. Özgür, L.; Akram, V.K.; Challenger, M.; Dağdeviren, O. An IoT based smart thermostat. In Proceedings of the 2018 5th International Conference on Electrical and Electronic Engineering (ICEEE), Istanbul, Turkey, 3–5 May 2018; pp. 252–256.

199. Tran, M.K.; Panchal, S.; Khang, T.D.; Panchal, K.; Fraser, R.; Fowler, M. Concept review of a cloud-based smart battery management system for lithium-ion batteries: Feasibility, logistics, and functionality. *Batteries* **2022**, *8*, 19. [CrossRef] [PubMed]

200. Boroojeni, K.G.; Amini, M.H.; Iyengar, S.S. *Smart Grids: Security and Privacy Issues*; Springer: Cham, Switzerland, 2017; Volume 221.

201. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]

202. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]

203. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]

204. Gönen, S.; Sayan, H.H.; Yılmaz, E.N.; Üstünsoy, F.; Karacayılmaz, G. False data injection attacks and the insider threat in smart systems. *Comput. Secur.* **2020**, *97*, 101955. [CrossRef]

205. Aydeger, A.; Zeydan, E.; Yadav, A.K.; Hemachandra, K.T.; Liyanage, M. Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In Proceedings of the 2024 15th International Conference on Network of the Future (NoF), Castelldefels, Spain, 2–4 October 2024; pp. 195–203.

206. Yılmaz, Y.; Uludag, S. Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *J. Frankl. Inst.* **2021**, *358*, 172–192. [CrossRef]

207. Berghout, T.; Benbouzid, M.; Muyeen, S. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100547. [CrossRef]

208. Chen, J.; Mohamed, M.A.; Dampage, U.; Rezaei, M.; Salmen, S.H.; Obaid, S.A.; Annuk, A. A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks. *Appl. Sci.* **2021**, *11*, 9972. [CrossRef]

209. Zhang, Y.; Wang, J.; Chen, B. Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach. *IEEE Trans. Smart Grid* **2020**, *12*, 623–634. [CrossRef]

210. Unsal, D.B.; Ustun, T.S.; Hussain, S.S.; Onen, A. Enhancing cybersecurity in smart grids: False data injection and its mitigation. *Energies* **2021**, *14*, 2657. [CrossRef]

211. Desai, S.; Sabar, N.R.; Alhadad, R.; Mahmood, A.; Chilamkurti, N. Mitigating consumer privacy breach in smart grid using obfuscation-based generative adversarial network. *Math. Biosci. Eng* **2022**, *19*, 3350–3368. [CrossRef]

212. Chehri, A.; Fofana, I.; Yang, X. Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability* **2021**, *13*, 3196. [CrossRef]

213. Bouyakoub, S.; Belkhir, A.; Bouyakoub, F.M.; Guebli, W. Smart airport: An IoT-based airport management system. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; pp. 1–7.

214. Pech, M.; Vrchota, J.; Bednář, J. Predictive maintenance and intelligent sensors in smart factory. *Sensors* **2021**, *21*, 1470. [CrossRef]

215. Andel, J.; Šimák, V.; Škultéty, F.; Nemec, D. IoT-based Data Acquisition Unit for aircraft and road vehicle. *Transp. Res. Procedia* **2021**, *55*, 969–976. [CrossRef]

216. Wang, X.k.; Liu, Y.y.; Li, Z.y.; Li, M.f.; Zhang, S.l. Aviation equipment maintenance safety management based on the technology of IOT. In Proceedings of the 19th International Conference on Industrial Engineering and Engineering Management: Engineering Management, Changsha, China, 27–29 October 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 1185–1194.

217. Okpala, I.; Parajuli, A.; Nnaji, C.; Awolusi, I. Assessing the feasibility of integrating the internet of things into safety management systems: A focus on wearable sensing devices. In Proceedings of the Construction Research Congress 2020: Computer Applications, Tempe, AZ, USA, 8–10 March 2020; American Society of Civil Engineers: Reston, VA, USA, 2020; pp. 236–245.

218. Noel, S.; Navya, M.; Likitha, D.; Manjula, K.; Priya, S.K. A Smart IoT based real-time system to Minimize Mishandled Luggage at Airports. In Proceedings of the 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 8–10 April 2021; pp. 377–384.

219. Samha, A.K.; Alghamdi, N.; Albader, H.; Alshammri, G.H. Applied Internet of Things in Saudi Arabia Airports. In Proceedings of the 2020 16th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2020; pp. 103–111.

220. Wang, J.; Feng, J.; Gao, Y.; Jiang, X.; Tang, J. A Intelligent Cabin Design Based on Aviation Internet of Things. In Proceedings of the 5th China Aeronautical Science and Technology Conference, Jiaxing, China, 3 November 2022; Springer: Singapore, 2022; pp. 963–969.

221. Jalali, R.; Zeinali, S. Smart Flight Security in Airport Using IOT (Case Study: Airport of Birjand). *Int. J. Comput. Sci. Softw. Eng.* **2018**, *7*, 142–147.

222. Aboti, C.D. Studies of Challenges to Mitigating Cyber Risks in IoT-Based Commercial Aviation. *Int. J. Sci. Res. Dev.* **2020**, *7*, 133–139.

223. Cho, S.H.; Park, S.Y. Reviewing the Utilization of Smart Airport Security. *J. Korean Soc. Aviat. Aeronaut.* **2023**, *31*, 172–177. [CrossRef]

224. Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-security challenges in aviation industry: A review of current and future trends. *Information* **2022**, *13*, 146. [CrossRef]

225. Florido-Benítez, L. Identifying cyber security risks in Spanish airports. *Cyber Secur. Peer-Rev. J.* **2021**, *4*, 267–291. [CrossRef]

226. Adhikari, S. Intelligent Cyber Defense in 5G Augmented Aviation Cybersecurity Framework. In Proceedings of the AIAA Scitech 2021 Forum, Virtual, 11–15 January 2021; p. 0661.

227. Zhang, C. Research on Transparency and Optimization of Aviation Materials Supply Chain based on Blockchain. In Proceedings of the 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT), Jabalpur, India, 6–7 April 2024; pp. 334–339.

228. Zkik, K.; Sebbar, A.; Nejjari, N.; Lahlou, S.; Fadi, O.; Oudani, M. Secure Model for Records Traceability in Airline Supply Chain Based on Blockchain and Machine Learning. In *Digital Transformation and Industry 4.0 for Sustainable Supply Chain Performance*; Springer: Cham, Switzerland, 2023; pp. 141–159.

229. Bitton, R.; Shabtai, A. A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1164–1181. [CrossRef]

230. Thales Group. IoT Cybersecurity: Regulating the Internet of Things. *THALES GROUP* **2024**. Available online: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations (accessed on 13 May 2024).

231. Lata, M.; Kumar, V. Standards and regulatory compliances for IoT security. *Int. J. Serv. Sci. Manag. Eng. Technol. (IJSSMET)* **2021**, *12*, 133–147. [CrossRef]

232. Open Connectivity Foundation. OCF Solving the IoT Standards Gap. *Open Connectivity Foundation* **2022**. Available online: https://openconnectivity.org/what-to-expect-from-an-interoperable-iot/ (accessed on 13 March 2023).

233. Open Connectivity Foundation. OCF Solving the IoT Standards Gap. 2023. Available online: https://openconnectivity.org/ (accessed on 25 April 2024).

234. Ye, W.; Heidemann, J.; Estrin, D. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Trans. Netw.* **2004**, *12*, 493–506. [CrossRef]