future internet

MDPI

Article

A Survey on Energy-Aware Security Mechanisms for the Internet of Things

Peixiong He [1], Yi Zhou [2,*] and Xiao Qin [1,*]

[1] Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA; pzh0029@auburn.edu
[2] TSYS School of Computer Science, Columbus State University, Columbus, GA 31907, USA
* Correspondence: zhou_yi@columbusstate.edu (Y.Z.); xqin@auburn.edu (X.Q.)

Abstract: The Internet of Things (IoT) employs sensors and the Internet for information exchange, enabling intelligent identification, monitoring, and management, which has deeply impacted various sectors such as power, medical care, and security, transforming social activities and lifestyles. Regrettably, IoT systems suffer from two main challenges, namely sustainability and security. Hence, pondering how to enhance sustainable and energy-efficient practices for IoT systems to mitigate risks becomes a worthwhile endeavor. To address this issue, we conduct a survey of energy-aware security mechanisms in the Internet of Things. Specifically, we examine the challenges that IoT is facing in terms of energy efficiency and security, and we inspect current energy-saving and privacy-preserving technologies for IoT systems. Moreover, we delineate a vision for the future of IoT, emphasizing energy-aware security mechanisms. Finally, we outline the challenges encountered in achieving energy-aware security mechanisms, as well as the direction of future research. Motivated by this study, we envision advancements in the IoT that not only harness the benefits of science and technology but also enhance the security and safety of our data.

Keywords: Internet of Things; energy saving; security

check for updates

Citation: He, P.; Zhou, Y.; Qin, X. A Survey on Energy-Aware Security Mechanisms for the Internet of Things. *Future Internet* **2024**, *16*, 128. https://doi.org/10.3390/fi16040128

Academic Editors: Olivier Markowitch and Jean-Michel Dricot

Received: 16 February 2024
Revised: 22 March 2024
Accepted: 31 March 2024
Published: 8 April 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the beginning of the industrial 4.0 era, human production and life have entered a completely new period—and the Internet of Things (IoT) interconnects numerous sensing devices through the Internet and improves industrial productivity by providing innovative technological facilities and intelligent services and applications [1]. During this period, IoT devices are capable of self-programming as well as collaborating among themselves, and the devices can accomplish computation, decision making, and control of data without access to cloud computing [2]. The proliferation of IoT has changed the way individuals interact with the world and leading-edge technology. From the smallest smartwatch to the rise of autonomous vehicles, from smart homes to the development of smart cities, the IoT has been playing a role in advancing the technology and civilization of human society [3]. The IoT technology has significant economic and environmental impacts thanks to the billions of connected devices communicating over the Internet using various types of sensors [4,5]. These connected devices imply large amounts of energy consumption and data management.

1.1. Motivation

Our research underpinnings are inspired by two motivations: (1) the importance of energy efficiency and (2) the critical issues of security and protection. Figure 1 illustrates the co-citation network of publications and their citation relationships for the period of 2019–2024. Among them, the topics of IoT, security, and energy are closely related. In order to provide a comprehensive survey and promote potential research in the area of an energy-efficient and secured IoT, we systematically present existing work on the energy-aware IoT

in terms of the way in which the IoT consumes energy and the available energy-saving technologies. Then, we sort the current challenges and future research directions for achieving high energy efficiency in the IoT. Finally, we combine existing technologies for an energy-efficient and secure IoT, and we conclude that seamlessly integrating energy-efficient computing and security is one of the future megatrends of the IoT.

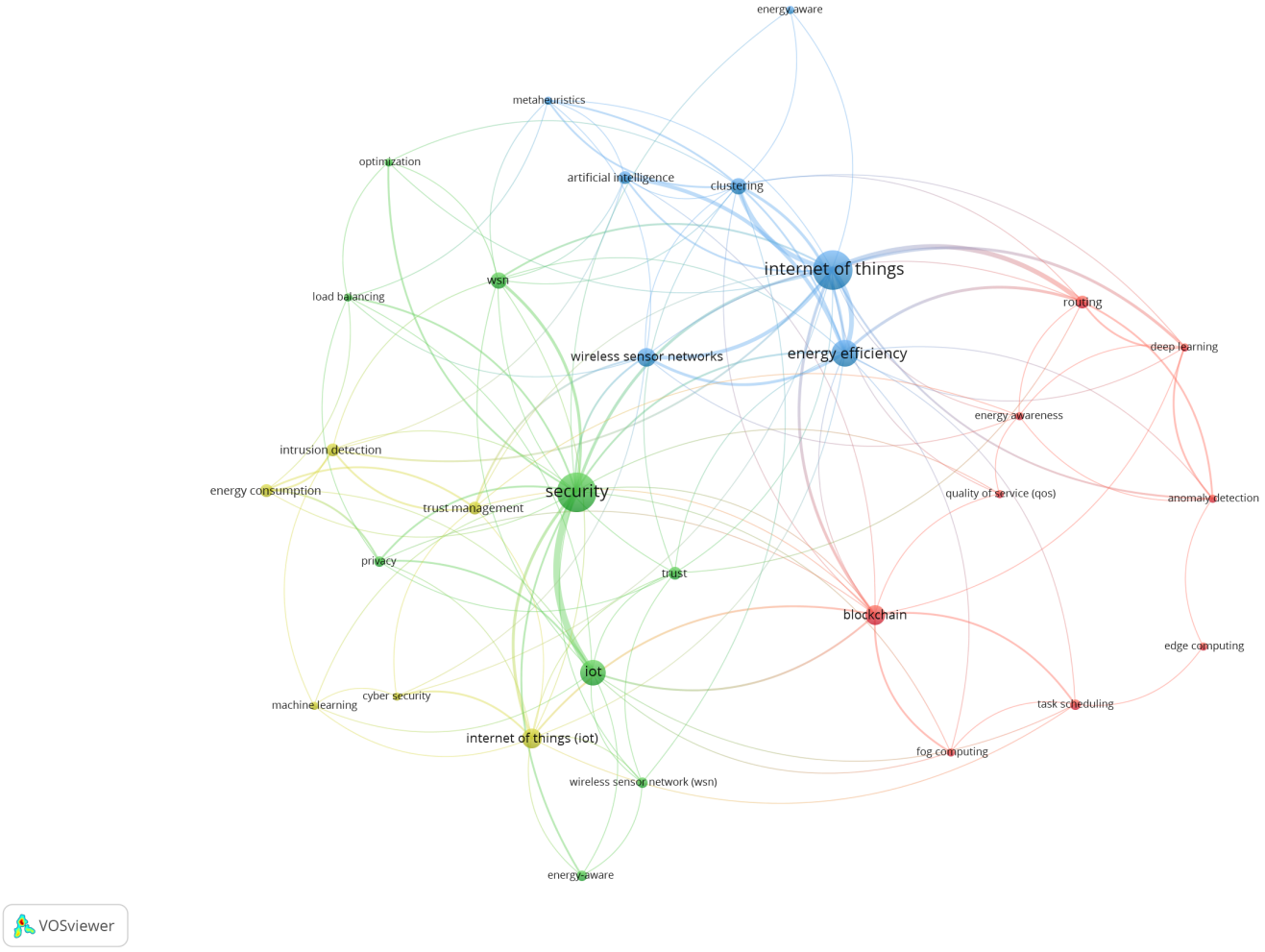

Figure 1. Visualization of the co-citation network of 'IoT', 'energy', and 'security' publications. Reference relationship from 2019–2024.

1.2. Importance of Energy Efficiency

More often than not, IoT devices are deployed remotely or in mobile environments—and the use of batteries to power IoT terminals has become the dominant paradigm today. While the use of batteries to power IoT terminals provides flexibility and independence for the devices, it also presents a number of challenges and drawbacks. First, the battery life limits the long-term operational capability of the device. After all, the battery life is limited, and with the passage of time, the battery capacity will gradually decrease, and providing convenient installation also means that the battery needs to be replaced periodically to ensure the normal operation of the sensor network. Frequently changing batteries increases the difficulty and cost of operation and maintenance. This greatly limits the growth rate of the Internet of Things. Imagine that when billions or even tens of billions of sensors are battery-powered, the labor and material costs of maintenance will become an unpredictable economic burden. According to a prior study [6], the size of IoT nodes will be limited—and hundreds of billions of nodes may not be deployed if batteries have to be regularly replaced. This not only leads to huge maintenance expenses,

but also has the potential to compromise at least 80% of the value of the IoT. Thus, battery replacement costs pose a significant challenge to the sustainability and economics of a large-scale IoT. Efforts to address this issue have focused on finding more durable and sustainable energy solutions, such as energy-harvesting technologies, long-life battery technologies, and wireless charging technologies, in order to reduce the pressure on battery maintenance costs.

Thanks to the advantages of lithium batteries such as a light weight and long life, they have now become the preferred power supply method for IoT sensors. However, with the increasing demand for batteries, the convenience brought by lithium batteries is accompanied by a series of problems. First, there are potentially toxic materials in lithium batteries, posing a serious threat to human health and the natural environment. Second, in order to produce lithium batteries, manufacturers need to mine large quantities of key raw materials such as lithium, cobalt, nickel, manganese, and graphite, a process that consumes large amounts of energy and water resources and often results in chemical pollution and geological damage to the local environment. In addition, batteries can accidentally release cobalt and copper during production and disposal, posing a direct risk to human health [7]. Therefore, despite the significant advantages of lithium batteries in providing energy, the benefits and drawbacks must be carefully weighed in the quest for a more environmentally friendly and sustainable energy sources.

In fact, most of the traditional sensors use batteries as the main energy supply method [8], which is obviously a huge consumption of human and material resources. Sensors, as an irreplaceable part of the Internet of Things, have a limited battery life to power them, and in order to guarantee the proper functioning of the sensor network, all batteries need to be replaced periodically to ensure that the sensors continue to operate properly. The battery life depends on factors such as the power consumption of the sensor, its operating frequency, and the parameters it measures. Hence, maintenance personnel need to check the status of the batteries—and periodic replacement prevents sensors from stopping working due to energy depletion. This manual maintenance inevitably involves cost and labor resources, and in some cases may result in temporary sensor failures until the batteries are replaced. In areas that are difficult to reach or require frequent monitoring, such a maintenance becomes more complex and expensive. Even worse, frequent battery replacement undermines the core value of connected sensors, and one of the main reasons that organizations deploy IoT sensors is that these devices can help them automate monitoring. If these sensors themselves continue to require regular human maintenance to ensure their proper functioning, then implementing automated monitoring makes far less sense.

1.3. Importance of Security Protection

IoT devices are widely used in industries such as healthcare, manufacturing, transportation, and smart homes because of the IoT's ability to provide features like intelligence, automation, and real-time monitoring to increase efficiency [9], reduce costs, and enhance the quality of life. However, it is these very same advantages that also make IoT devices a major target for hackers, because IoT devices—being deployed on a large scale—cover a wide range of applications. This nature gives attackers ample opportunities to locate potential targets, so it is of paramount importance to implement cyber security solutions to safeguard these devices.

Similarly, data security is at the core of information security. In today's world of increasingly advanced intelligence, data-faking techniques based on smart science pose a huge challenge to information security. This challenge is demanding because healthcare devices may contain the sensitive medical data of patients, manufacturing devices may store production processes and trade secrets, and transportation and smart home devices may involve the personal information of users. If an attacker obtains this critical information, and conducts theft, extortion, or other malicious activities leading to the violation of personal privacy, or in more serious cases, even the leakage of confidential information, then offering strong data security is important to securely protect the user information.

IoT devices play an important role in critical infrastructures, such as medical devices, transportation-control systems, and manufacturing processes. Attackers may cause service disruptions through malicious operations [10], which can have a significant impact on society and the economy. The security of the Internet of Things is more of a precursor to the protection of critical infrastructure, which is directly related to the infrastructure of the economic operation, social order, and public interest, and has a significant impact on the information system, including communications, electric power, water conservancy, transportation, finance, energy, and municipal and other areas of the various networks, as well as information infrastructures and important information systems. Once a critical information infrastructure is damaged, loses its functions, or has a data leakage, it may seriously jeopardize national security, economic operations, and the social order, and even cause widespread social panic. Therefore, safeguarding the security of IoT infrastructures is a top priority for national security and social stability.

1.4. Contributions

This study of energy-aware security mechanisms provides an effective solution to the conflict between the security and energy efficiency of IoT devices. Compared with existing research, we comprehensively examine multiple dimensions such as hardware, software, network, and data management, summarize the main contributions of the current research results in terms of the two key themes of energy efficiency and security, and provide an in-depth analysis of the presence of potential problems. It also provides new perspectives and ideas for subsequent research on energy-aware security mechanisms, which will help promote the sustainable development of IoT technologies. This survey will help future researchers apply energy-aware security mechanisms in real IoT systems.

1.5. Organization

The remainder of this paper is organized as follows, see Figure 2. In Section 2, we introduce several energy consumption factors in the IoT, challenges in realizing IoT energy efficiency, existing IoT energy-saving technologies, and emerging trends and future directions in energy-efficient computing for the IoT. In Section 3, we discuss the evolving IoT threats, analyze the defense layer of IoT security from multiple dimensions, and reflect on the challenges and future directions of IoT security. Next, in Section 4, we take a look at energy-aware security mechanisms in the IoT, and summarize ways of making the energy-security trade-offs in the IoT, the challenges of implementing energy-aware security mechanisms, and the approaches to achieving energy-aware security. We elaborate on case studies and examples of energy-aware security mechanisms, as well as discuss their directions and related open research questions. Finally, the last section presents concluding remarks.

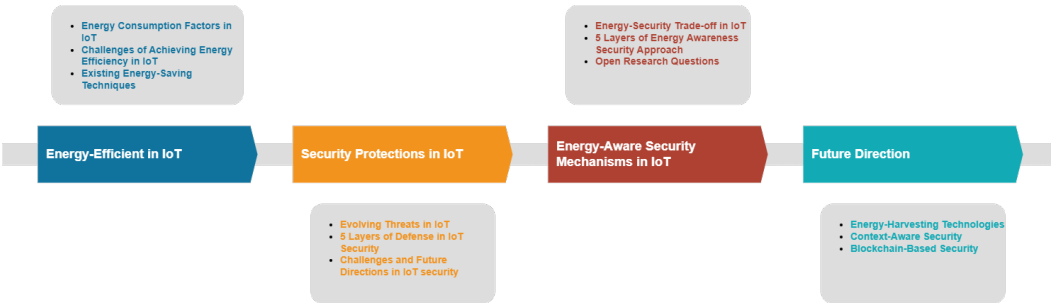

Figure 2. The graphical abstract of this paper.

2. Energy-Efficient IoT

2.1. Energy Consumption Factors in the IoT

We will now delve into the energy consumption factors in the IoT (see Figure 3), which are categorized as follows:

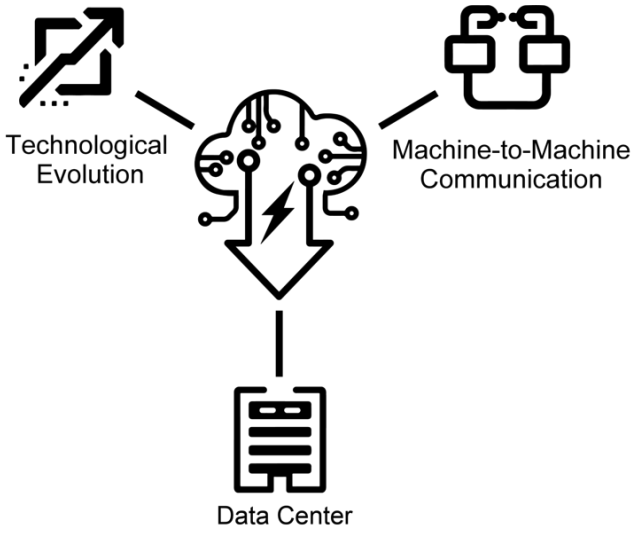

Figure 3. Energy-consumption factors in IoT systems.

2.1.1. Data Centers

IoT devices, equipped with sensors, cameras, and other components, generate a large amount of data collected from their environments [11], which is then transferred to data centers, becoming a critical source of input for servers, storage devices, and cooling systems. Such a process ultimately poses a huge strain on existing infrastructure, including cloud data centers [12]. Consequently, data centers must constantly undergo upgrades and expansions to meet the increasing demand for servers, storage devices, and cooling systems. Unfortunately, the constant upgrades not only lead to a high energy consumption in data centers but also cause additional environmental and economic costs. To address this issue, rethinking how to achieve higher energy efficiency and mitigate the over-reliance on power resources in data centers becomes indispensable.

2.1.2. Machine-to-Machine (M2M) Communication

Communication protocols in the IoT, such as short-range LAN communications, cellular networks, and satellite communications, ensure the real-time data transmission between devices. However, these communication protocols also pose various energy-management challenges. For example, communication operations, signal transmission, and network maintenance all place significant demands on power resources. WiFi or Bluetooth technologies used in LAN communications, as well as cellular networks and satellite communications on a wider scale, require stable communication connectivity, which places tremendous demands on power resources. This power demand phenomenon becomes more severe in machine-to-machine (M2M) communication scenarios, where 'smart devices' communicate with each other autonomously and make collaborative decisions without human intervention [13]. Even worse, since these devices are battery-powered and often require constant and uninterrupted connections, frequent charging becomes inevitable, thereby leading to increased energy costs. Therefore, carefully managing the charging cycles of devices is essential to maintaining reliable yet high-speed data transmission while minimizing power consumption.

2.1.3. Technological Evolution

The rapid development of IoT technology makes device renewal and iteration inevitable. As technology continues to advance, replacing old devices with new ones results in excessive e-waste. In addition to the potential environmental threat posed by the e-waste generated by equipment obsolescence, the disposal process also induces energy resource demands [14]. Meanwhile, producing, configuring, and deploying new-generation equipment also leads to

transitional energy waste. Though it is an inevitable part when embracing new technologies, we need to provide energy-efficient strategies during device-renewal processes.

A variety of strategies can be utilized to effectively reduce energy consumption in the IoT. For instance, optimizing data-processing algorithms can reduce the burden on data centers, thereby reducing energy consumption. Energy-efficient communication technologies can help slash the amount of power support required for communications. The use of renewable energy in the manufacturing and operation of IoT devices can decrease the reliance on non-renewable energy sources, thereby enhancing overall energy sustainability. In addition, sustainable update strategies for devices are conductive to mitigating energy demands caused by device renewal. Moreover, energy-efficient hardware and software technologies can be introduced to further enhance the energy efficiency of IoT devices and thus reduce energy costs. Lastly, holistic approaches can be leveraged to enhance IoT energy efficiency and achieve the goal of sustainable development.

2.2. Challenges of Achieving Energy Efficiency in the IoT

In this part of the study, we discuss the challenges of realizing energy efficiency in the IoT as follows:

2.2.1. Resource Constraints

Resource constraints, such as processing power, memory capacity, and communication bandwidth are major challenges to achieving energy efficiency in the IoT domain. IoT devices are often equipped with processors with limited computing power (industrial sensors or sensor nodes, RFID tags, etc.) [15], making it difficult to perform complex tasks. For example, the limited memory capacity of these devices restricts the amount of data they can store and process, which has implications for energy efficiency. This challenge is particularly critical in application scenarios that require IoT devices to process large amounts of data in real-time [16]. Similarly, IoT applications, like smart cities, environmental monitoring, and health monitoring, require quick data processing to provide real-time feedback and decision support. However, due to the limitations of processing power, these devices often need to offload complex data analysis tasks to cloud- or edge-computing platforms. This not only increases the data transmission latency and energy consumption but also raises concerns about data privacy and security.

2.2.2. Heterogeneity

The heterogeneity of the IoT poses multiple obstacles to achieving energy efficiency. IoT environments typically consist of a wide variety of devices, technologies, platforms, and protocols [17]. Although this heterogeneity provides configuration flexibility for various applications, it also brings about issues such as integration complexity, interoperability, management, and security. For example, IoT systems are normally comprised of different types of devices like sensors, smart cameras, air pollution monitors, communication protocols, and others [18]; as a result, these devices differ broadly in design and functionality, energy consumption, and battery life. Such differences make it complicated to implement a generic energy-saving strategy.

2.2.3. Dynamic Atmospheres

IoT devices are often deployed in dynamic environments, where their operating conditions and network statuses are constantly changing [19]. This dynamism significantly influences the effectiveness of energy management strategies: first, IoT devices transmitting data rely on networks, the quality and availability of which fluctuate depending on the location, time, and other factors. Second, high network latency or low bandwidth environments may compel devices to make multiple attempts to transmit data, thereby increasing energy consumption [20]. Third, an IoT device may switch its operating state, such as transitioning from a low-power mode to a high-power mode, according to current operational

requirements [21]. Therefore, it is obvious that adjusting the states of IoT devices in a timely manner while meeting performance requirements becomes increasingly challenging.

2.3. Existing Energy-Saving Techniques

Energy-saving technologies for the IoT are defined from five main perspectives: hardware, software, network protocols, data management, and machine learning. See Figure 4.

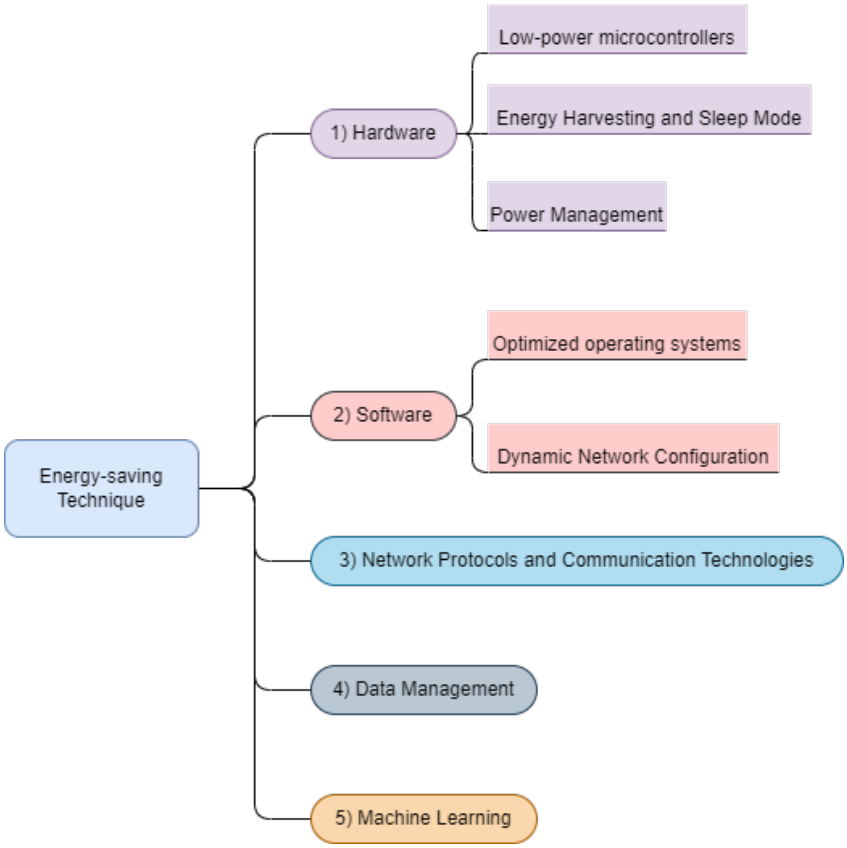

Figure 4. Existing energy-saving techniques.

2.3.1. Hardware Energy-Saving Techniques

- *Low-power microcontrollers.* Low-power microcontrollers in IoT systems considerably extend the battery life, making them ideal for applications that require long runtimes. Due to the fact that sensor nodes are often battery-powered in reality, lowering the energy consumption not only extends battery life but also reduces battery replacement needs, which in turn slashes the risk of environmental contamination when discarding old batteries [22]. Additionally, energy savings yielded by low-power microcontrollers help cut back the demand for power resources.
- *Energy Harvesting and Sleep Mode.* Energy harvesting technologies refer to the processes that capture and convert external energy sources into electrical energy. There exists a broad spectrum of external energy sources, including solar, mechanical, thermal, wind, water, radio frequency, etc. For example, solar energy-harvesting technologies strive to leverage solar cells to convert light energy into electrical energy, whereas radio-frequency energy-harvesting technologies harness radio frequency signals to perform electrical energy conversion. On the other hand, the development of sleep-mode technologies becomes essential to achieve long-term self-sustainability for IoT applications [23]. Taking a sensor node as an example, if there is no need for it to sense its target environment for a certain period of time, it can transition to sleep mode for energy-saving purposes. Likewise, its sensors can be transitioned to sleep mode if its battery power drops below a critical threshold. The transitions can be

performed dynamically based on multiple factors such as the sensors' battery status and information quality. In short, energy-harvesting and sleep mode technologies help extend devices' life and enhance the energy utilization of IoT systems [24].

- *Power Management.* Advanced power-management techniques, such as power-curtailment strategies and dynamic voltage and frequency scaling (DVFS), can effectively diminish power consumption. Power-curtailment strategies (e.g., power-gating techniques) focus on reducing the static power consumption of digital circuits. The power consumption of digital circuits consists of two main contributors: dynamic power consumption and static power consumption. Dynamic power consumption refers to the power consumed when the circuit is switched, while static power consumption is primarily due to the leakage current of the transistors, which consumes power even when the circuit is not performing any operation [25]. The power-gating technique inserts control switches between different parts of a circuit such that the power supply to a block of circuitry will be cut off when the block has no task to perform, thereby reducing the power consumption of digital circuits [26]. As for DVFS, it is a commonly used strategy that dynamically adjusts the power voltage and clock frequency of processors. In particular, in underload conditions, DVFS lowers a processor's voltage and frequency to reduce the power consumption. Conversely, in overload conditions, DVFS increases the processor's voltage and frequency to provide necessary computing power [27]. This technique is especially critical for battery-powered mobile devices because it enables IoT devices to achieve the best performance-to-energy ratio under various workload conditions, thereby prolonging their service time. In brief, power-management techniques fine-tune the power supply to IoT systems, reducing the overall power consumption of IoT devices and extending the battery life of battery-powered devices.

2.3.2. Software Energy-Saving Techniques

- *Optimized operating systems.* IoT devices often utilize specifically designed lightweight operating systems (e.g., Contiki and TinyOS) to enhance the operation efficiency and reduce system overhead [28], satisfying the needs of resource-constrained environments. For instance, an optimized operating system can intelligently switch an IoT device between sleep and active modes to reduce the power consumption when it sits in an idle state for a certain period, thereby effectively improving the energy efficiency of the device.
- *Dynamic Network Configuration.* Dynamic network configuration can improve the energy efficiency of IoT devices through communication optimization [29]. It allows IoT devices to make adjustments according to changing network conditions, such as the signal strength, network load, and interference. Such adaptability enables IoT devices to operate with minimal energy consumption under various conditions. For example, reducing the frequency of data transmission when a network signal is weak can reduce the power consumption. This example signifies that a dynamic network configuration not only lowers the energy consumption but also mitigates network congestion.

2.3.3. Network Protocols and Communication Technologies

Communication technologies, such as low-power WiFi, Bluetooth low energy (LE) [30], and low-power wide area network (LPWAN) [31], were developed to minimize energy consumption, making them ideal for IoT applications that require a long battery life. WiFi HaLow [32], one of the low-power WiFi versions, constructed based on the IEEE 802.11ah standard [33] features high data transmission efficiency so as to diminish power consumption. Bluetooth LE, characterized by short communication intervals and quick connection establishment, reduces the power consumption while maintaining stable communication. LPWAN technology, allowing long-distance communication (several kilometers), reduces

the need for multiple relays or access points, making it suitable for long-range and low-data rate scenarios.

2.3.4. Data-Management Technology

Data aggregation refers to the process of combining multiple data sources or sensors into a single unified data set. Data aggregation lessens the power consumption required for communication by reducing the amount of data transmitted. In-network processing, on the other hand, strives to reduce the energy consumption by processing data at the edge of a network, with only the necessary information or processing results being sent to the cloud.

2.3.5. Optimizing Machine Learning

Machine learning algorithms can dynamically adjust equipment power settings and forecast equipment failures, based on real-time conditions and historical information, thereby harvesting energy savings. For example, by intervening before the occurrence of equipment problems and preventing equipment from running in an inefficient or lossy state, the use of machine learning algorithms can yield energy savings. Likewise, machine learning is capable of fine-tuning the equipment runtime and task scheduling, aligning the energy consumption closely with the real demand.

2.4. Emerging Trends and Future Directions

The new trends and future directions for the energy-aware IoT involve a number of areas, including energy harvesting, artificial intelligence, and regional blockchains.

2.4.1. Energy Harvesting

New materials and technologies: recently, energy-harvesting technologies, such as flexible solar cells, thermal energy-harvesting materials, and vibration-based technologies have emerged [34]. Tiny energy sources in the environment, such as differences in light and temperature, are harnessed by flexible nanogenerators and thermal energy converters to generate electricity. Meanwhile, device vibration or motion is utilized by vibration-based energy-harvesting technologies to generate electricity for wireless sensors and wearable devices.

2.4.2. Artificial Intelligence

Machine learning and artificial intelligence show promise for optimizing the resource allocation and data collection in IoT systems. Edge computing and edge AI can make local real-time decision making feasible for IoT devices and thus reduce their reliance on cloud services, thereby lowering the power consumption for communications and cloud computing. AI-powered data analysis can also facilitate optimizing energy management such that IoT devices can operate intelligently and efficiently.

2.4.3. Blockchain

Blockchain technology is demonstrating great potential in pursuing a sustainable future [35]. This is mainly attributed to its trait of decentralized, secure, and transparent data-management mechanisms. Blockchain technology, through its real-time monitoring capabilities, creates ample opportunities to implement appropriate energy-saving measures. In particular, the combination of edge computing, which processes data closer to data sources to reduce the data transmission time and latency, with the goal of reducing energy consumption, ensures security and transparency. Advances in these emerging areas will stimulate continued innovation in energy-efficient IoT technologies, making IoT systems smart, sustainable, and secure.

3. Security Protections in IoT Environments

Along with the rapid development of the IoT industry, IoT attacks—such as privacy leakage, illegal invasion, and local network damage—become frequent. It is expected that

with the further expansion of the scale of the IoT, the destructive power of attacking the IoT will be further expanded, and the IoT security issues are increasingly becoming a concern of the society. The following is a more detailed discussion of cyber-threats to IoT devices. In Section 3.1, we will discuss a variety of cyber-threats that target IoT devices. Next, we will elaborate on layers of defense in IoT security in Section 3.2.

3.1. Evolving Threats in the IoT

We start this part with the introduction of denial of services. Then, we articulate IoT security issues such as data breaches and physical manipulation. Finally, we discuss three vulnerabilities of IoT devices.

3.1.1. Denial of Service Attacks (DoS)

A Denial of Service (DoS) attack (see Figure 5) is a cyber attack that makes a website or service unavailable by overwhelming the system with an enormous amount of requests from multiple sources [36]. A Distributed Denial of Service (DDoS) attack [37] is a special type of DoS attacks that utilizes a network of compromised devices, called a botnet, to send attack requests. Such swift DoS and DDoS attacks are difficult to defend against and therefore, their consequences are highly destructive. In DDoS attacks, web servers are flooded with a large number of requests for replies to the message, consuming network bandwidth or system resources, resulting in overloaded networks or systems where normal services stop providing [38]. DDoS manifests itself in two main forms, namely flow-of-traffic attacks [39] and resource-exhaustion attacks [40].

- *Flow-of-Traffic Attacks.* Under this type of attacks, the network bandwidth is blocked by a large number of malicious packets that overwhelm legitimate traffic. These attacks aim to exhaust the network's capacity to handle data, effectively denying service to legitimate users.
- *Resource-Exhaustion Attacks.* The focal point of these attacks is the server itself, which receives a multitude of attack packets that deplete memory or CPU resources. Such attacks aim to prevent servers from processing legitimate requests, leading to a denial of service.

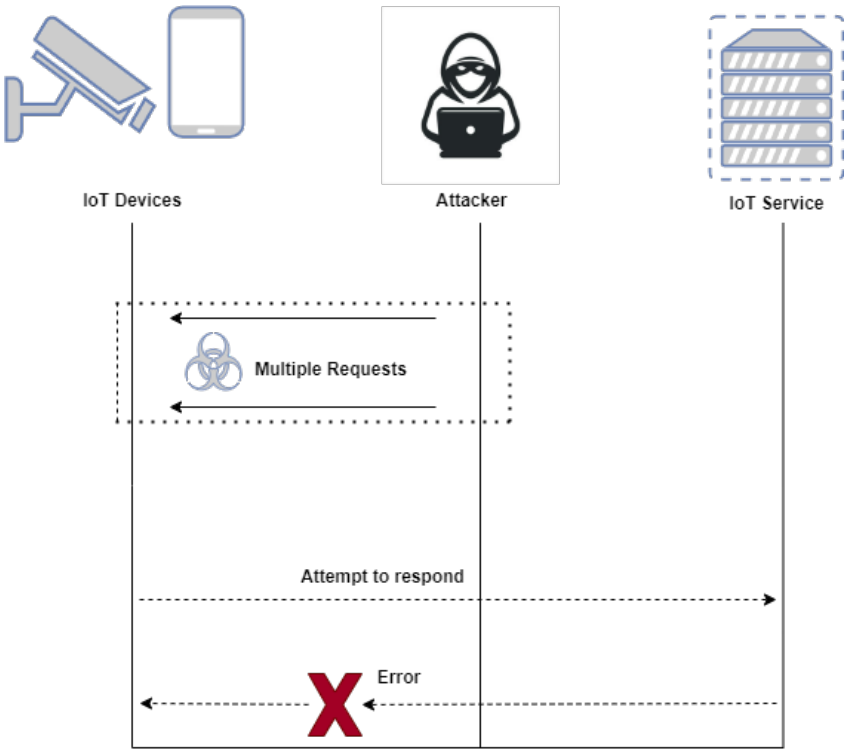

Figure 5. Denial of service attack in IoT systems.

3.1.2. Botnets, Data Breaches, and Physical Manipulation

Attackers often infect and control thousands, if not millions, of computers to form a large *botnet* that is capable of launching DDoS attacks, large-scale spam campaigns, or other types of cyberattacks. Data breaches in DDoS are security incidents that involve both the exposure of confidential or sensitive information and the disruption of the availability or performance of a website or service [41]. When attackers use malware to infect IoT devices, the attackers do more than just adding the device to a botnet. For example, cyberattackers can access device data and steal sensitive information stored in it, and the attackers also use IoT to obtain credentials from device firmware. Using these credentials, the attackers access corporate networks or other systems storing sensitive data. In this way, an attack on these devices could turn into a full-blown data breach.

Attacks mainly targeting sensing devices may result in the leakage of sensitive information or malicious tracking. Since IoT devices are deployed in distributed remote environments, hackers are able to access and tamper with the physical layer, obtain sensitive information, and interrupt services furnished by IoT devices. Because IoT devices are used in most IoT applications such as smart homes and smart healthcare, it is crucial to protect them from IoT attacks. In cases of product failure or any kind of cyberattacks on these devices, the device systems and the life of users will be seriously affected.

3.1.3. Unique Vulnerabilities of IoT Devices

Now let us analyze the unique vulnerabilities of IoT devices from the following three perspectives, namely weak authentication [42], insecure communication protocols [43], and outdated firmware [44].

- *Weak Authentication.* Weak authentication in IoT devices, like unchangeable default passwords, opens doors for attackers to seize control of entire networks.
- *Insecure Communication Protocols.* Insecure communication protocols, similar to weak authentication, leave users vulnerable to data theft and manipulation attacks by acting as open doors for hackers, especially on public WiFi networks.
- *Outdated Firmware.* Outdated firmware and limited update capabilities in IoT devices create easy openings for hackers, leaving networks vulnerable to known software attacks.

Authentication technology is the most direct and cutting-edge line of defense in network security, and is an important means of preventing illegal invasion and virus damage. Many IoT devices have weak authentication mechanisms [45], such as default passwords or simple passwords, and users rarely change these passwords, thereby making IoT systems vulnerable to unauthorized accesses. Weak credentials, coupled with limited authentication methods, create opportunities for attackers to compromise devices and gain control of IoT networks.

As with weak authentication by default, insecure communication protocols allow hackers to intercept traffic or perform network "snooping" to easily view sensitive data traveling over the networks. This issue makes systems and devices vulnerable to man-in-the-middle (MITM) attacks [46], and one of the most common methods of MITM attacks is through public WiFi, which often has insecure communication protocols allowing an attacker to gain access to information from any devices connected to the network. The attacker can even lure the user to a fake server that has been set up in advance so as to conduct illegal activities such as fraud against the user.

IoT devices often have limited computing resources, and may lack appropriate mechanisms for regular firmware updates and security patches. As a result, these devices often run on outdated and vulnerable versions of software. Hackers actively exploit known vulnerabilities in outdated firmware to gain unauthorized access to, or control of, IoT devices. The lack of a streamlined process for providing timely updates and patches to IoT devices poses a significant challenge, as it exposes devices and networks to attacks that could be prevented.

3.2. Layers of Defense in IoT Security

A multilayered approach to ensuring the security of IoT devices and systems is a comprehensive challenge. Due to the large number of IoT front-end devices dispersed in unattended environments, the devices are highly susceptible to attacks and exploitation, resulting in the inability of core business systems to operate normally.

The IoT security requirements are mainly reflected in the following three layers of IoT systems.

- *Device Layer.* This layers contains a massive amount of sensors and control devices—such as sensors and control devices—deployed on sites.
- *Communication Layer.* The second layer provides a variety of communication protocols coupled with interfaces to realize functions such as data collection, device control, and system maintenance.
- *Application Layer.* This layer is comprised of a cloud platform performing the comprehensive configuration, operation and management of IoT terminals like smart grids and telemedicine.

In what follows, we discuss today's defense strategies for the IoT three-layer architecture from five aspects: device (see Section 3.3), network (see Section 3.4), software (see Section 3.5), application (see Section 3.6), and management (see Section 3.7). Figure 6 provides an overview of common threats in the IoT and corresponding defenses.

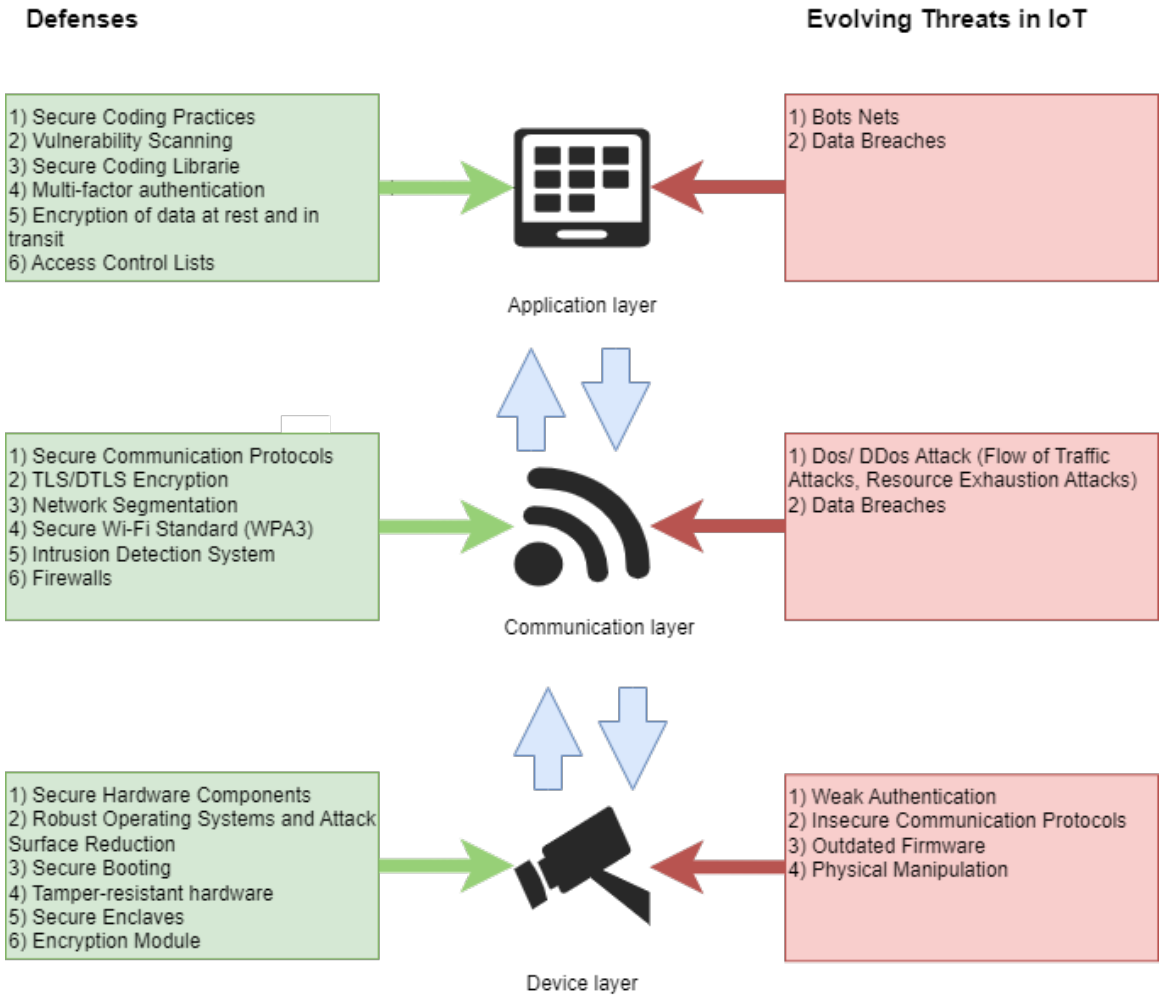

Figure 6. Common threats in the IoT with corresponding defenses.

3.3. Defense at the Device Layer

3.3.1. Secure Hardware Components

The selection of secure hardware components is critical to the overall security of IoT devices [47]. Microcontrollers are the core components of embedded systems, and microcontrollers specifically designed to enhance security can be selected to improve the security of a device. Similarly, hardware security modules [48] (*HSMs*) are widely used in scenarios in which IoT devices are protected by securely managing, processing, and the storing of cryptographic keys and digital certificates. HSMs are widely used in venues (e.g., such as financial services, data protection, and enterprise security) where security is highly desired. HSMs offer robust protection for encryption keys by utilizing dedicated secure cryptographic processors. These processors can be housed within plug-in cards (SAM/SIM cards) or external devices connected directly to computers or web servers. The key discrepancy of HSMs lies in their tamper-resistant design: this often includes a physically secure enclosure that automatically deletes stored keys upon unauthorized physical access, preventing key disclosure. In essence, HSMs offer a secure environment for the entire lifecycle of an encryption key, safeguarding IoT systems from various threats.

3.3.2. Robust Operating Systems and Attack Surface Reduction

In IoT environments, adopting an operating system with strong security and minimizing the attack surface is a key strategy for protecting devices from threats. It is wise to elect an operating system designed specifically for IoT security, and examples for OSs optimized for IoT devices include FreeRTOS, RIOT OS, and Zephyr [49]. These operating systems are usually designed to be lightweight and include only the necessary functional modules to reduce the potential attack surface. More importantly, unnecessary system services and applications, especially those that may listen to network ports or provide remote access capabilities, are disabled or removed from the operating systems. In these scenarios, system processes and applications are running with elevated privileges to mitigate the risks of being maliciously exploited.

3.3.3. Secure Booting

Secure booting is critical to prevent attackers from compromising operational IoT programs [50], because any malicious code inserted into a device could make that device part of a botnet. For example, an attacker may implant a local device with a file containing malware. If the device is not protected by a secure boot, the malicious code will execute on the next reboot to compromise the device. With the secure boot process, security checks during reboots identify unauthorized executables, prevent any threats from running, and enable the associated protections.

3.3.4. Tamper-Resistant Hardware

Choosing hardware devices equipped with built-in detection capabilities [51] makes it possible to recognize and respond to any form of physical tampering attempts. This strategy is a precaution that is especially important for IoT devices storing sensitive information or that control critical infrastructure, which, if tampered with, could pose a serious threat to personal privacy or public safety.

3.3.5. Secure Enclaves

Secure enclaves use specialized hardware controls used to securely isolate data and instructions at the CPU level [52]. Such an isolation is furnished by strong cryptography that verifies the authenticity of the enclave while offering privacy and integrity of the enclave code and the sensitive data being processed.

3.3.6. Encryption Module

Encryption modules at the hardware level are a technology specifically designed to realize data encryption and decryption operations on physical devices. These modules

implement encryption algorithms through hardware rather than software, enhancing both security and performance. A good example is the trusted platform module, or TPM [53]—a hardware encryption module that is widely deployed in computing devices. A TPM can securely store encryption keys, digital certificates, and other sensitive data. Through these features, the TPM is capable of delivering strong hardware-level security services. Hardware-level security mechanisms provide a higher level of protection than software encryption because the hardware-level mechanisms are more difficult to compromise by remote hackers or software vulnerabilities. By integrating TPMs during the design and manufacturing phases of a device, users and organizations can establish a strong security foundation in IoT environments.

3.4. Defense at the Network Level

3.4.1. Secure Communication Protocols

Network security is an important aspect of end-to-end IoT security. As devices communicate with one another and with assorted cloud services, it is critical to ensure the secure transmission of data and prevent unauthorized access. This protection can be achieved by using secure communication protocols, such as datagram transport layer security (DTLS), to furnish secure communication among IoT devices [54].

In the network layer security, encrypted communication is seen as the cornerstone of securing data transmission [54]. This is achieved through the use of strong encryption algorithms such as transport layer security (TLS) or a secure sockets layer (SSL) [55] for secure website accesses (HTTPS) [56], and other network services that require a secure channel [57]. The network-level defense aims to ensure that data are not intercepted or tampered with during transmission and that mutual authentication is implemented between the client and server.

Although the TLS and DTLS protocols share the same goal of securing data in transit, they are each applicable to different network protocols and scenarios. TLS—a standard encryption protocol dedicated to providing communication security—is primarily used on TCP (transmission control protocol) [58] connections to offer security protection for the communication between web browsers and servers, e-mail, instant messaging, and other services. DTLS is a variant of TLS designed for the UDP (user datagram protocol). Since the UDP is a connectionless protocol, it is mainly used in applications that require high-speed transmission and low latency such as video conferencing. DTLS facilitates TLS-like security in these situations, including encryption, authentication, and data integrity protection.

3.4.2. Network Segmentation

Network segmentation is an effective means of improving network security [59]. Users may apply virtual local area networks (VLANs) [60], IP address ranges, and combinations to divide the network into smaller local networks. This strategy allows users to forge multiple security zones and represent different segments controlled by firewalls. Network segmentation reduces overall system risks, and facilitates rapid response and recovery by assuring that the data and resources in each segment are visible and accessible only to authorized users in the current segment.

3.4.3. Intrusion-Detection/Prevention Systems (IDS/IPS)

Evidence demonstrates that intrusion-detection systems (IDS) and intrusion-prevention systems (IPS) are essential for detecting and responding to network attacks [61]. An IDS is a technology used in network security to detect and identify suspicious activity [62]. When suspicious behavior or activity that violates security policies are detected, the IDS generates and sends an alert to administrators or to an integrated security information and event management (SIEM) system [63].

There are two main types of IDSs, namely network intrusion-detection systems (NIDSs) and host intrusion-detection systems (HIDSs) [64]. NIDSs are mainly deployed at network boundaries or data-center entrances to monitor all the network traffic passing through and

detect potential malicious activities or violations, whereas HIDSs are installed on specific hosts or servers to monitor the system logs, file system changes, and detect attacks or abnormal behaviors.

Firewalls—the first line of defense against compromise—shield IoT devices from unauthorized access and malicious traffic, and by configuring the firewall, system administrators can limit the ports and services that are accessible, allowing only the necessary communications to effectively reduce the attack surface. For example, Cisco's enterprise firewall solutions empower organizations with advanced network security, including intrusion prevention and unified communications protection, safeguarding critical data and ensuring seamless communication [65].

3.4.4. Secure WiFi Standard (WPA3)

Adopting the latest WiFi security standards, such as WPA3, helps in bolstering the security of WiFi networks. WPA3 introduces the simultaneous authentication of equals (SAE) algorithm, which replaces the pre-shared key (PSK) authentication used in WPA2 [66]. SAE enhances the password security and improves resistance to brute-force breaking attacks, especially against dictionary attacks. In addition, WPA3 utilizes a higher level of encryption and provides a 192-bit encryption key, whereas WPA2 only supports a 128-bit encryption key. WPA3 is suitable for the government, financial, and medical industries that require high data security. Additionally, WPA3 provides perfect forward secrecy, ensuring that even if a long-term key is compromised, previous communication data remain secure: an attacker cannot access past communications by decrypting captured packets.

3.5. Defense at the Software Level

Software-level defense is an efficient approach to building robust and secure IoT systems. Continuous attention to security throughout the software development lifecycle and the adoption of appropriate defenses are key to ensuring that the software remains secure in the face of evolving threats. In what follows, we articulate the defense at the software level from the perspectives of secure coding practices (see Section 3.5.1), vulnerability management (see Section 3.5.2), and access control and data storage (see Section 3.5.3).

3.5.1. Secure Coding Practices

Secure coding practices are a critical part of the software-development process designed to guide developers on how to write more secure code [67]. These practices are designed to reduce the vulnerability of software and systems to security breaches, thereby protecting applications from attacks. Examples include using strong hash functions like Argon2, bcrypt, or PBKDF2 [68] to store user passwords, and employing salt to further enhance security.

Common security threats and vulnerabilities that can be protected by secure coding practices include memory security and buffer overflows. This method requires developers to use safe functions when coding, avoiding functions such as *strcpy()* and *sprintf()* that are known to cause problems [69].

Regularly reviewing code [70] is the process of checking source code to pinpoint and eliminate vulnerabilities or errors that are likely to compromise security in software. The code-reviewing process ensures that the implemented code meets the security standards and complies with the industry regulations. This practice not only helps to enhance the code quality and performance but also prevents potential attacks by hackers.

Using secure coding libraries coupled with software frameworks with embedded security is an effective way to improve the quality and security of code during software development (see Figure 7). These libraries provide a collection of rigorously vetted and tested code modules that enable developers to avert insecure code practices. Common secure coding libraries and frameworks that prevent security vulnerabilities include OWASP ESAPI, Spring Security, and Microsoft SDL. Figure 7 lists a set of example secure coding

libraries, frameworks, and patches, which are devised to help software developers to implement security features throughout the development lifecycle [71].

Classes	Names	Types	Description
Cryptography	OpenSSL	Library	Provide cryptographic functions: TLS/SSL, X.509 certificates.
	BoringSSL	Library	It is smaller, faster, and more secure than OpenSSL.
	NaCl	Library	Offer a small set of well-vetted cryptographic primitives.
Web Security	OWASP AntiSamy	Library	Prevent XSS attacks by sanitizing user input.
	OWASP ESAPI	Library	Provides input validation, output encoding, and session management.
	Spring Security	Framework	Offer security features: authentication, authorization, and session management.
System Security	SELinux	MAC System	Allow administrators to define fine-grained security policies.
	AppArmor	MAC System	Allow administrators to define fine-grained security policies.
	Grsecurity	Patches	Security patches for the Linux kernel to be resistant to attacks.

Figure 7. A list of sample secure coding libraries, frameworks, and patches, which enable developers to build robust and secure IoT systems.

3.5.2. Vulnerability Management

Vulnerability management is a necessary measure to secure software [72]. Vulnerability management allows for an effective update policy to ensure that the device's firmware and software are kept up to date, reducing the risk of known vulnerabilities. For example, security patches are pushed to devices through a remote update mechanism after the product's release.

Regular vulnerability scanning helps to find and fix potential vulnerabilities in software [73]. Network application layers are regularly scanned for vulnerabilities, and any discovered vulnerabilities are fixed in a timely manner to optimize the security of the IoT device.

3.5.3. Access Control and Data Storage

Strict access controls in the facility limit software and system access. The risk of unauthorized access can be avoided by implementing the principle of least privilege, user authentication, and authorization. For example, IoT systems assign user-specific access permissions based on their roles, ensuring individuals access only to job-relevant information.

Strong data-storage practices, including encryption, access control, and regular backups, safeguard sensitive information, preventing breaches and minimizing the risk of theft, leaks, and associated consequences. An example is the use full-disk encryption like BitLocker [74] to encrypt the contents of the entire hard drive. For the complete security of IoT systems equipped with data storage, users should leverage robust encryption options like MySQL's AES function and SQL Server's transparent data encryption [75].

3.6. Defense at the Application Level

We will now shed light on the security practices and defenses at the application level, which facilitates the secure authentication of user identity and protects the secure transmission of sensitive data. By combining multi-factor authentication (see Section 3.6.1), data encryption (see Section 3.6.2), and access control (see Section 3.6.4), more robust and secure IoT applications can be built.

3.6.1. Secure User Authentication

The first line of defense at the application level is, of course, the use of secure user authentication. Applying strong password policies, multi-factor authentication, and the like can ensure that only authorized users are allowed to access applications, thus safeguarding IoT devices from malware infections and other security threats. In doing so, systems verify that only authorized users are allowed to access specific data or IoT device functions. This authentication technique prevents unauthorized access and operations and improves system security.

To improve security, an increasing number of IoT systems adopt multi-factor authentication, or MFA [76]—a mechanism that combines passwords, biometrics, and other authentication methods. This security approach greatly enhance the level of security, making it difficult for intruders to gain access through simple password guessing or stealing.

3.6.2. Data Security APIs

By using secure application program interfaces (APIs), it is possible to make data transfers between applications safe and secure. Data security APIs enable data signatures and integrity checks to confirm that data have not been tampered with during the storage or transmission phases [77]. IoT systems can verify data integrity by the virtue of hash functions and digital signatures, guaranteeing the systems' authenticity and reliability.

Figure 8 tabulates a list of popular data security APIs along with their descriptions and security features.

APIs	Description	Authentication and Access Control	Enterprise Grade	Monitor	Data Security
Amazon Cognito	User authentication, authorization, and management	✓			
Auth0	Passwordless authentication and social logins	✓			
Azure Active Directory	Cloud-based identity and access management	✓	✓		
Fortanix Data Security Fabric	Encrypted key management service, access control	✓			✓
Google Cloud Identity Platform	Cloud-based identity and access management	✓	✓		
IBM Guardium Data Encryption	Data encryption and access control for databases	✓	✓		✓
McAfee Data Loss Prevention	Data loss prevention and endpoint security		✓	✓	
Okta	Secure user access management	✓	✓		
OneLogin	Identity and access management (IAM) solution	✓	✓		
Palo Alto Networks Prisma Cloud	Protect data in cloud environments, detect and prevent data breaches			✓	✓

Figure 8. A list of sample data security APIs and their security features.

3.6.3. Encryption of Data at Rest and in Transit

Encryption of data at rest and in transit are two important concepts in data security that can be implemented at the application level. Data-at-rest encryption refers to the encryption of data stored on a device or server so as to protect the data from unauthorized access [78]. This type of encryption prevents data breaches even if IoT devices are stolen or data are illegally accessed.

Data-in-transit encryption refers to the process of encrypting data when the data are being transmitted over a network, or "in transit", between two IoT systems [79]. Encryption of data in transit is a fundamental way of protecting sensitive information from interception and eavesdropping attacks in IoT environments.

3.6.4. Access Control Lists

Access control lists (ALCs) define at the device level which users or systems are authorized to access a particular IoT device [80]. This scheme-preconditioned access control ensures that device operations and data access are limited to authorized individuals, thus reducing the chance of malicious accesses by adversaries.

Role-based access control, or RBAC, is a flexible access-control model that assigns appropriate privileges to users anchored on their roles [81]. With the RBAC model in place, sensitive data and device features are only available to any roles that need the information. This highly centralized privilege control effectively alleviates the risk of data leakage and unauthorized accesses. Even if a user's credentials are compromised, a threat actor can only gain access to resources allowed by that user's role, thereby mitigating security risks.

3.7. Defense at the Management Level

A wide range of security practices and defenses at the management level assure that IoT devices and systems maintain a high level of security throughout the lifecycle. Evolving security threats can be effectively addressed through timely configurations (see Section 3.7.1), firmware updates (see Section 3.7.2), patch management (see Section 3.7.3), and effective incident responses (see Section 3.7.4).

3.7.1. Secure Supply and Configuration

Secure supply and configuration play a crucial role as they directly affect the security and reliability of IoT devices and their data. Devices with secure provisioning should have authentication as a feature, which ensures that each device can be uniquely identified and its identity can be verified [82]. This is important for establishing secure communication between devices. In addition, the corresponding security provisioning can configure the necessary minimum privileges for the devices and the applications running on them to reduce the attack surface. There are also configurations for firewalls, intrusion-detection systems.

3.7.2. Firmware Updates

Firmware updates are the most directly useful for patching known security vulnerabilities [83]. As software vulnerabilities continue to be discovered on IoT devices, regular firmware updates can patch these vulnerabilities in a timely manner. In addition to patching vulnerabilities, firmware updates also introduce new security features and enhancements, such as improved encryption algorithms, stronger authentication mechanisms, and enhanced data protection. These updates strengthen the device's resistance in the face of unknown attacks.

Given firmware updates, the device is able to verify that the firmware was released from a trusted source. This advantage prevents malware or firmware from being injected by untrusted third parties, thereby avoiding the risk of the device being infected with malicious code [84]. Firmware updates are completed using encryption (typically public/private key encryption). When a device receives a firmware update, it verifies the signature using the publisher's public key. This process ensures that the firmware has not been tampered with during transmission, thus protecting the integrity of the firmware update.

3.7.3. Patch Management

One of the main roles of patch management is to patch security vulnerabilities in a timely manner to prevent attackers from exploiting them for unauthorized access or malicious attacks. Additionally, regular patch management can ensure that the software and firmware running on the IoT system are kept up to date, ensuring the overall stability of the IoT system [85].

Patch management systems furnish a systematic approach to offering timely updates and maintenance of device firmware and software: the management systems automatically identify and apply security patches to fix known vulnerabilities [86]. This automated process minimizes the likelihood of human error and ensures that vulnerabilities are swiftly patched before being widely exploited, thus protecting IoT devices and networks from attacks.

3.7.4. Incident Response

Incident-response mechanisms help to quickly detect and respond to security threats, and through real-time monitoring and alerting systems, security teams can detect threats at an early stage and take swift action to mitigate damage [87]. Moreover, the security team can analyze the security incident and propose follow-up improvement measures, such as fixing vulnerabilities, improving security policies and processes, and strengthening defenses to prevent similar incidents from happening again.

Incident response plans require a pre-defined set of processes and procedures designed to guide the response of security personnel when faced with a security incident. These plans are key to ensuring a quick and effective response to security threats, minimizing damage and restoring normal operations [88]. Additionally, a high-security incident response plan categorizes and prioritizes detected events to ensure that high-priority events are responded to quickly, which can greatly minimize the negative impact of security events on the IoT environment, while promoting the organization's ability to adapt to and resist future threats.

3.7.5. Security Configuration Protocols

The use of secure configuration protocols helps ensure that devices are initialized and configured with optimal security settings. By defining and enforcing security configuration standards, the exposure of devices to threats caused by configuration errors can be reduced [89]. The Arms Security Configuration Protocol ensures that only authorized users and devices have access to the network and data by implementing strong authentication and authorization mechanisms and secure communication protocols such as SSL/TLS.

3.8. Challenges and Future Directions in IoT Security

3.8.1. Challenges

The security challenges of the IoT are indeed multifaceted, especially due to its wide range of application scenarios and diverse device types. Some of these challenges include resource constraints, device heterogeneity, and a lack of standardization. Meanwhile, in the face of these challenges, future research directions present many promising areas, including lightweight encryption, AI-driven security, blockchain-based security, and privacy-preserving technologies.

- *Resource Constraints.* Many IoT devices have limited processing power, memory, and communication bandwidth, which limits the possibility of implementing robust security measures on these devices. Therefore, designing security solutions that adapt to resource-constrained environments is a challenge.
- *Heterogeneity of Devices.* There are various types of devices in the IoT that may have different operating systems, processor architectures, and communication protocols. Harmonizing security standards and mechanisms for these heterogeneous devices is a complex task.
- *Lack of Standardization.* The lack of unified IoT security standards and specifications makes it more difficult to develop comprehensive security policies and implementation strategies. The lack of standardization may lead device manufacturers and service providers to take different approaches to security.

3.8.2. Future Directions

The following research and innovation to be undertaken as future directions will overcome the aforementioned challenges to IoT security, and lay the foundation for a robust and trusted IoT ecosystem.

- *Lightweight Encryption.* Lightweight encryption algorithms for resource-constrained devices are a key future direction for IoT security. These algorithms need to secure data while minimizing the impact on device performance to improve the overall security of the IoT system [90]. Efficient and lightweight authentication is also one of the future directions of security research, which is important because verifying the identity of the user prevents sensitive data leakage and improves the performance of IoT networks.
- *Artificial Intelligence-Driven Security.* Traditional encryption methods are often utilized to address security and privacy issues in IoT networks; however, the nature of IoT nodes makes it impossible for existing methods to support the architecture of an entire complex and large IoT network, in part due to resource constraints and the large amount of real-time data generated by IoT devices. One may apply machine learning

and deep learning solutions to IoT devices and networks, aiming to optimize the overall security of the system by learning statistical information collected from sensors. For instance, IoT systems may adopt deep learning to train a model that automatically identifies malicious behaviors to improve the self-protection performance.

- *Blockchain-based Security.* Blockchain technology provides decentralized and tamper-proof data management, which is suitable for security and tamper-proof requirements in the IoT. Thus, the blockchain ensures trust between devices and provides traceable data records that help prevent data tampering and malicious access and can effectively protect customers from data privacy breaches [91].
- *Privacy-Protection Technologies.* IoT devices provide personalized services by collecting and analyzing user data, which poses the risk of privacy leakage. Therefore, the future development of IoT security will inevitably focus more on privacy-protection techniques.

4. Energy-Aware Security Mechanisms in IoT

With the rapid growth of IoT systems, sensitive data protection and secure operation in IoT systems become essential to guard against potential cyber-threats. Another challenge requiring special attention is energy efficiency in resource-limited IoT devices and networks. In this regard, the notion of energy-aware security not only cuts back energy consumption but also supplies an effective means for maintaining security in resource-constrained IoT environments.

4.1. Energy–Security Trade-off in the IoT

There is an intrinsic conflict between security and energy efficiency in resource-constrained IoT systems. Traditional security approaches usually require intensive computation and communication, including complex cryptographic algorithms, key management, and authentication processes, which conflict with the energy efficiency of IoT devices. High energy-consuming operations desire frequent battery replacements, which is a non-negligible factor for jeopardizing the battery life of IoT devices. As IoT devices are widely deployed, this issue will exacerbate the high energy consumption of IoT devices, harming network infrastructure. Therefore, taking into account factors of energy consumption and device lifetime becomes indispensable when designing sustainable yet secure IoT systems.

4.2. Challenges of Implementing Energy-Aware Security

The implementation of energy-aware security in IoT systems is facing several challenges. First, resource constraints have emerged as a primary concern. For example, security algorithms running on IoT devices must be energy-efficient, since IoT devices typically are equipped with relatively limited computing power and storage capacity. Second, the heterogeneity discussed above poses a challenge to applying targeted security policies to an entire IoT system consisting of various devices of different functionality. Third, environmental dynamics and uncertainty compel IoT devices to operate in unpredictable and harsh environments, which require security mechanisms to be capable of securing devices under diverse conditions. Fourth, modern IoT systems must feature real-time monitoring and response, as well as quick adaption to cope with evolving cyber-threats. Therefore, gaining in-depth insights into these challenges for implementing energy-aware security mechanisms in IoT systems is desired to provide guidelines for further growth.

4.3. Approaches to Energy-Aware Security

The design principle of energy-aware security aims to minimize power consumption while ensuring system security for IoT systems. We outline the implementation of energy-aware security from five perspectives: hardware, network, software, application, and management. Figure 9 list an overview of the approaches we provide to future energy-aware security mechanisms.

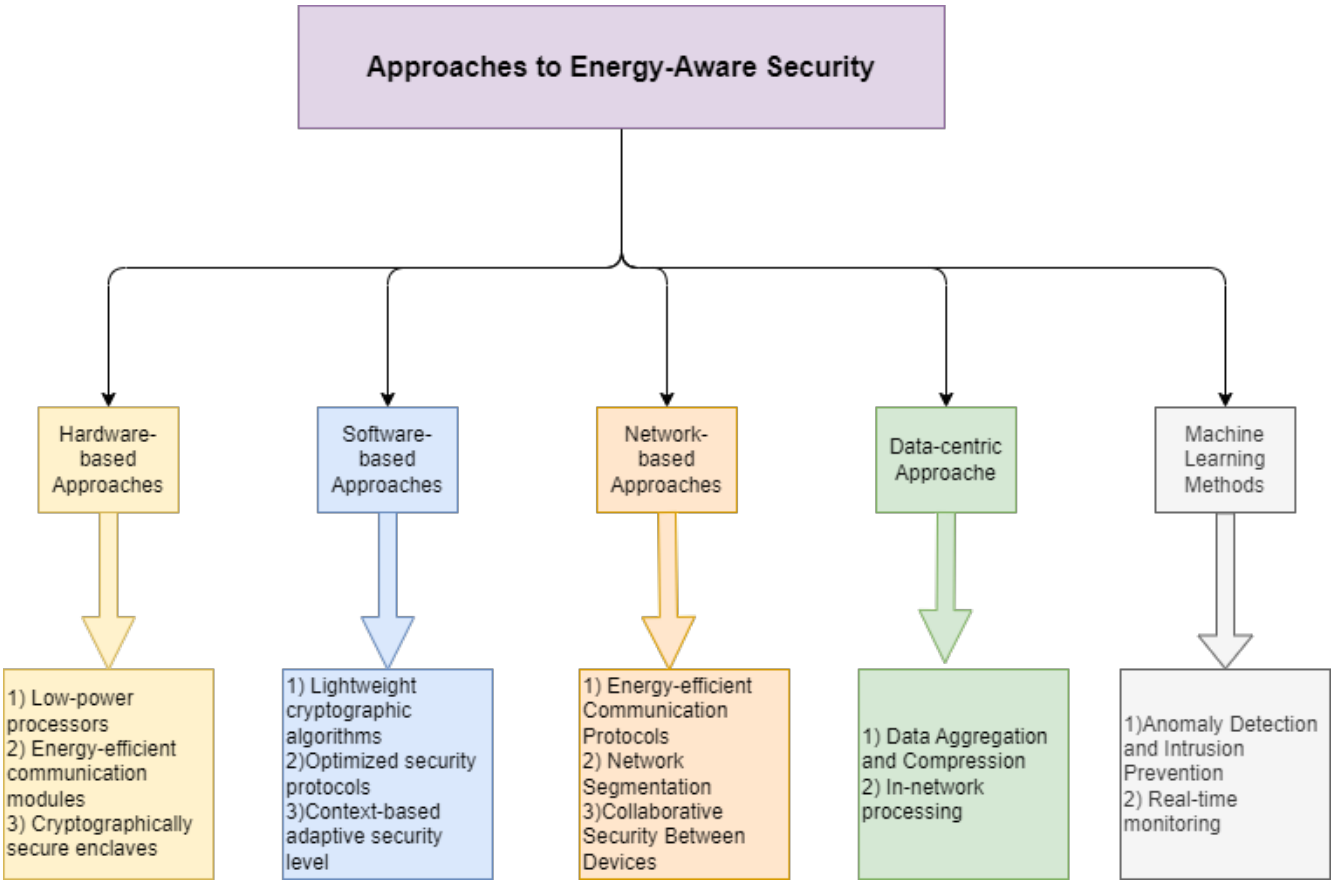

Figure 9. An overview of approaches to energy-aware security.

4.3.1. Hardware-Based Approaches

- *Low-power processors.* Low-power processor design aims to reduce the power consumption at an acceptable cost of performance degradation [92], which is widely used in mobile devices, as well as wearable and embedded systems. With low-power processors in place, devices gain longer battery life and better energy efficiency.
- *Energy-efficient communication modules.* Energy-efficient communication modules aim to reduce the power consumption of security operations, thereby ensuring security while achieving overall energy efficiency [93].
- *Cryptographically secure enclaves.* Cryptographically secure enclaves allow encryption and decryption operations to be executed efficiently at the hardware level. Applications executing in a secure enclave can reduce the demand for repetitive security checks and data encryption operations, thereby diminishing the power consumption.

4.3.2. Software-Based Approaches

- *Lightweight cryptographic algorithms.* Lightweight encryption algorithms are designed to utilize fewer computational resources when performing encryption and decryption operations to lower power consumption. This is extremely important for battery-powered devices, as these devices can perform security operations with a reduced amount of time and a lower energy consumption [94].
- *Optimized security protocols.* Optimized security protocols that require less computation can diminish the power consumption when performing security-related tasks. For example, security protocols for specific low-power communication standards, such as Bluetooth low-energy (BLE) security, can ensure secure communication with minimal energy consumption [95].
- *Context-based adaptive security levels.* Encryption algorithms that adaptively adjust the strength according to security requirements and energy availability are conducive

to achieving energy efficiency [96]. Specifically, When network conditions are stable or the data transmitted are non-sensitive, energy-efficient communication methods will be adopted. Conversely, when sensitive data need to be transmitted, secure but energy-intensive protocols will be utilized. Likewise, lower-strength encryption will be utilized in low-risk environments to conserve energy, whereas strong encryption algorithms will be adopted in high-risk environments to ensure data protection.

4.3.3. Network-Based Approaches

- *Energy-efficient Communication Protocols.* Energy-efficient communication protocols reduce packet sizes during data transmission to cut back on energy consumption. These protocols leverage effective data compression algorithms to diminish the number of communications. In addition, energy-efficient communication protocols harness optimized security mechanisms, such as lightweight encryption algorithms and efficient key management systems, for low-power environments.
- *Network Segmentation.* Network segmentation refers to monitoring and maintaining each segment independently in terms of security assurance. This security simplification facilitates reducing computational and communication activities, which in turn lowers power consumption.
- *Collaborative Security Between Devices.* Collaborative security mechanisms remove unnecessary security checks and response activities via information sharing and the collaborative analysis between devices, thereby conserving energy. Devices can also share security-processing tasks, such as distributed intrusion detection, to eliminate the burden on individual devices and thus remove power consumption.

4.3.4. Data-Centric Approaches

- *Data Aggregation and Compression.* This allows for data-processing tasks to be performed locally, thereby reducing data transmission, data leakage risks, network congestion, and power consumption.
- *In-network processing.* In-network processing reduces the amount of data transmitted to processing nodes over a network and thus conserves energy consumed for the communication between nodes.

4.3.5. Machine Learning Methods

- *Anomaly Detection and Intrusion Prevention.* Supervised learning algorithms can be used to identify types of attacks with high accuracy, whereas unsupervised learning algorithms are able to detect unknown, untagged attacks and anomalous behaviors. Pierpaolo et al. [97] demonstrated the outstanding effectiveness of machine learning (ML) models in identifying attacks, particularly in the realm of anomaly detection (binary classification) and anomaly classification (multi-class issues).
- *Real-Time Monitoring.* Based on historical energy usage data, ML models can be trained to identify patterns of energy wastage to facilitate designing energy-aware security policies. Additionally, ML models deployed on IoT devices can monitor incoming data streams to detect security threats in real-time while minimizing power consumption. For example, in IoT systems powered by federated learning algorithms, raw data are kept locally, with only model parameters transmitted to a central server or other devices (see Figure 10). By keeping sensitive data on local devices, federated learning reduces the risk of data leakage or unauthorized access, as well as the energy required to transfer large amounts of data [98].

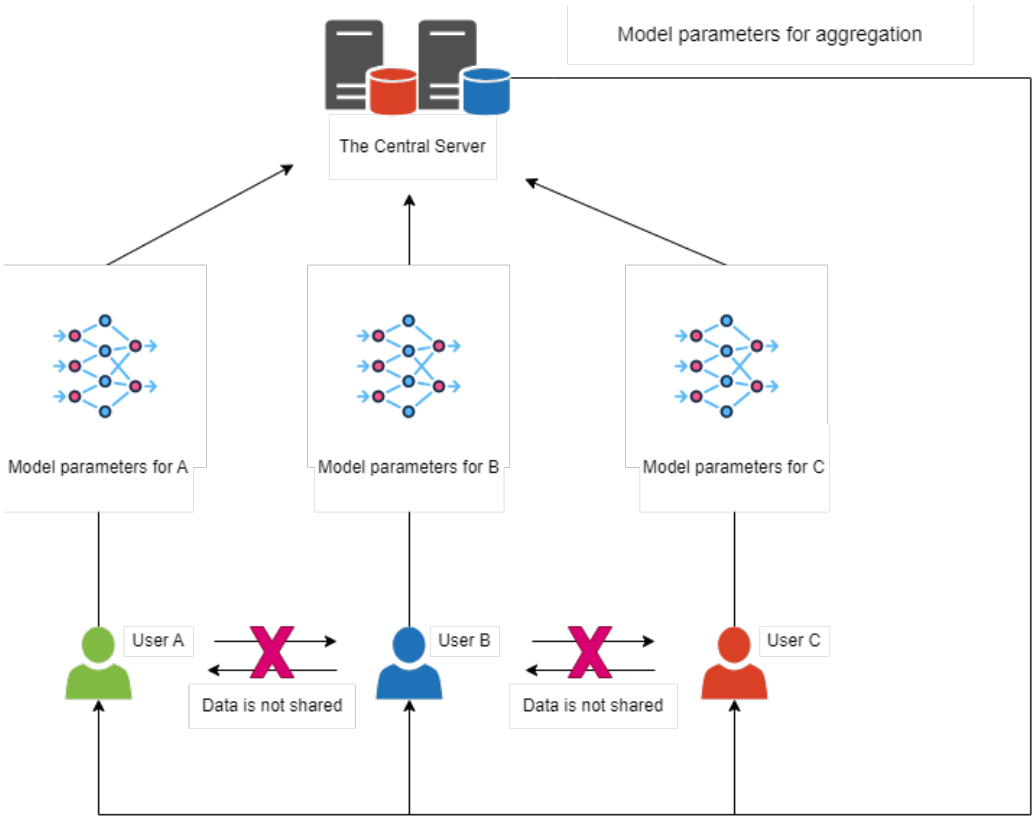

Figure 10. The structure of federated learning.

4.4. Case Studies

Bluetooth low-energy (BLE) technology finds extensive application in wearable devices. For example, Fitbit's wearable health tracker employs lightweight encryption to safeguard the transmission of user data, utilizing low-power Bluetooth (BLE) technology for synchronizing data with smartphones. Sports watches offer high-precision GPS tracking while maximizing battery usage through dynamic adjustments to the GPS frequency and the use of energy-efficient secure communication protocols.

Lightweight encryption algorithms are widely used in smart home devices, especially in resource-constrained devices, to strike a balance between security and energy efficiency. For example, the Advanced Encryption Standard (AES) is a symmetric block cipher scheme used to protect sensitive data [99], which is broadly employed in smart door locks. A smart door lock automatically enters sleep mode when the door is closed, and it wakes up only upon receiving a legitimate unlock command [100]. SimpliSafe, one of the most popular home security systems on the market today, employs secure TLS and elliptic curve encryption to protect video transmissions. Its cameras reduce power consumption by entering a low-energy standby state when no motion is detected [101].

Industrial sensors reshape the "sensing system" in Industry 4.0; improving the energy efficiency and security capabilities of sensing systems greatly stimulates IoT systems to progress toward the goal of energy-aware security. Intelligent industrial sensing has the capability to analyze, evaluate, and even adaptively learn to perform complex tasks, including image recognition, feature detection, and multi-dimensional detection. For example, Chingping et al. [102] proposed a sensor interface device crucial for sensor data acquisition in industrial wireless sensor networks (WSNs). This device utilizes a complex programmable logic device (CPLD) as the core controller application. CPLDs as the core controller greatly streamline the design of peripheral circuits and reduce the current consumption. Moreover, by adhering to the IEEE 1451.2 Smart Sensor Interface Specification standard [102], it ensures the secure and efficient acquisition of data from a variety of sensors, which is crucial for maintaining safety and promoting energy efficiency in industrial automation processes.

4.5. Future Directions and Open Research Questions

We delineate future research directions and open research questions in IoT energy-sensing security as the following emerging trends and promising areas (see Figure 11).

Figure 11. The future of energy-aware security in the IoT.

4.5.1. Energy-Harvesting Technologies

Given the necessity for future IoT devices to be more sustainable, energy-harvesting technologies will be a pivotal area of focus. Energy-harvesting technology is an environmentally friendly and innovative solution that extends the working life of sensors and, in some scenarios, can even completely replace traditional battery-powered methods. By optimizing the energy consumption and reducing the network maintenance costs, energy-harvesting technology offers both economic benefits and practical advantages [23]. Researchers will investigate methods to harness energy sources in the environment, such as solar, wind, and thermal energy, to deliver long-term stable power to devices. Emerging energy-harvesting materials, efficient conversion technologies, and strategies for integration with IoT devices to reduce the dependence on conventional batteries will also garner increased research attention.

4.5.2. Context-Aware Security

In the constantly changing environment of the IoT, context-aware security policies address the changing threats and challenges by utilizing contextual information about the surrounding environment to make security decisions [103]. Dynamic and smarter security measures should be proposed in response to dynamic changes in device states, environmental conditions, and threat levels. Sensors are the bridge for IoT devices to interact with the external environment, such as temperature, humidity, light, and motion, which can be used to collect context-awareness information. This involves assessing the context around the device in real-time through sensing technologies (e.g., image recognition, sensor data) and adapting security policies accordingly. For example, this includes increasing the level of security in high-risk environments while reducing power consumption in low-risk environments.

4.5.3. Blockchain-Based Security

Implementing secure and tamper-proof data-management systems with a minimal energy overhead will facilitate future breakthroughs in IoT security through the utilization of blockchain technology. The decentralized nature of the blockchain and its distributed

ledger will offer enhanced data protection, particularly concerning secure data transfer and authentication among IoT devices [104].

4.5.4. Standardization and Interoperability

With the growing number of IoT devices, standardization and interoperability become increasingly crucial. E-learning in particular illustrates the predictability of this perspective: as IoT wearable devices such as smartwatches are widely used in education, it will be essential to establish strict security and privacy standards to ensure that all relevant devices and programs adhere to these privacy guidelines. In addition, the interoperability of IoT systems is demonstrated through the use of intelligent whiteboards and virtual reality (VR) technologies that enhance the interactivity of the learning experience and emphasize the value of seamless integration across devices and platforms [105]. Future research will concentrate on creating common frameworks and protocols to guarantee the efficient resource utilization across various IoT systems. This involves aligning security standards, communication protocols, and interoperability standards among devices to streamline complexity across the IoT ecosystem and enhance the system's overall security. These emerging trends will offer innovative solutions for energy-aware security in the IoT and propel the entire field toward greater intelligence, sustainability, and security.

Open research questions encompass balancing the costs and benefits of energy-harvesting technologies, addressing security challenges in dynamically changing environmental contexts, and striking a balance between flexibility and consistency in the standardization process. Exploring these questions will pave the way for future research directions, advancing the development of IoT energy-sensing security.

5. Concluding Remarks

5.1. Conclusions

While commonly used IoT applications enhance efficiency, automation, and convenience across various domains of life and industry, the future direction and current challenges in the IoT remain unclear. To this end, in this survey, we examined two critical factors—security and energy efficiency—affecting the utilization of the IoT. We explored the challenges that the IoT is encountering in these two domains. We scrutinized current solutions and technologies aimed at addressing these challenges. Moreover, we outlined a vision for the future of the IoT, emphasizing energy-aware security mechanisms. More specifically, we elaborated on the challenges encountered in realizing energy-aware security mechanisms, as well as the motivations and directions of future research.

Inspired by our vision of energy-aware security mechanisms, we aspire for advancements in the IoT to offer us the benefits of science and technology, while enhancing the security and safety of our data.

5.2. Limitations and Future Work

Although this paper provides a comprehensive overview and analysis of the application of security techniques in Internet of Things (IoT) systems, it must be acknowledged that there are some limitations. First, given the breadth and complexity of the IoT security domain, we have yet to be able to fully explore other essential specialized security techniques such as key management, information flow, and security audit. These techniques play an important role in protecting information systems from unauthorized access and data leakage. At the current stage, our review does not visually compare and evaluate the performance of existing methods in terms of energy-saving efficiency and safety by means of mathematical statistics, and we aspire that future studies will analyze and assess the proposed safety and energy-saving techniques in more depth, including but not limited to experimental validation and performance testing. In addition, the diverse application scenarios of the IoT imply that new energy-efficient technologies and strategies will continue to emerge, and we will continue to focus on emerging energy-efficient technologies and further explore the dynamic relationship between energy efficiency and security, in par-

ticular, we will aim to propose a framework on how to achieve higher energy efficiency without sacrificing security.

Author Contributions: Conceptualization—P.H., Y.Z. and X.Q.; writing original draft preparation—P.H.; original idea, review and editing—Y.Z. and X.Q. All authors have read and agreed to the published version of the manuscript.

Funding: Xiao Qin's work is supported by the National Aeronautics and Space Administration (Grant 80NSSC20M0044), the National Highway Traffic Safety Administration (Grant 451861-19158), the U.S. National Science Foundation (Grants IIS-1618669 and OAC-1642133), and Wright Media, LLC (Grant 240250).

Data Availability Statement: Data are contained within the article.

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

References

1. Malik, P.K.; Sharma, R.; Singh, R.; Gehlot, A.; Satapathy, S.C.; Alnumay, W.S.; Pelusi, D.; Ghosh, U.; Nayak, J. Industrial Internet of Things and its applications in industry 4.0: State of the art. *Comput. Commun.* **2021**, *166*, 125–139. [CrossRef]
2. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *J. Syst. Archit.* **2019**, *98*, 289–330. [CrossRef]
3. Miller, M. *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*; Pearson Education: London, UK, 2015.
4. Memić, B.; Džubur, A.H.; Avdagić-Golub, E. Green IoT: Sustainability environment and technologies. *Sci. Eng. Technol.* **2022**, *2*, 24–29. [CrossRef]
5. Georgakopoulos, D.; Jayaraman, P.P. Internet of things: From internet scale sensing to smart services. *Computing* **2016**, *98*, 1041–1058. [CrossRef]
6. Harrop, P. *Battery Elimination in Electronics and Electrical Engineering 2018–2028*; IDTechEx: Cambridge, UK, 2017.
7. Mrozik, W.; Rajaeifar, M.A.; Heidrich, O.; Christensen, P. Environmental impacts, pollution sources and pathways of spent lithium-ion batteries. *Energy Environ. Sci.* **2021**, *14*, 6099–6121. [CrossRef]
8. Raj, A.; Steingart, D. Power sources for the internet of things. *J. Electrochem. Soc.* **2018**, *165*, B3130. [CrossRef]
9. Tien, J.M. Internet of things, real-time decision making, and artificial intelligence. *Ann. Data Sci.* **2017**, *4*, 149–178. [CrossRef]
10. 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]
11. Puschmann, D.; Barnaghi, P.; Tafazolli, R. Adaptive Clustering for Dynamic IoT Data Streams. *IEEE Internet Things J.* **2017**, *4*, 64–74. [CrossRef]
12. Ullah, R.; Ahmed, S.H.; Kim, B.S. Information-centric networking with edge computing for IoT: Research challenges and future directions. *IEEE Access* **2018**, *6*, 73465–73488. [CrossRef]
13. Chen, M.; Wan, J.; Li, F. Machine-to-machine communications: Architectures, standards and applications. *Ksii Trans. Internet Inf. Syst.* **2012**, *6*, 480–497. [CrossRef]
14. Gaidajis, G.; Angelakoglou, K.; Aktsoglou, D. E-waste: Environmental problems and current management. *J. Eng. Sci. Technol. Rev.* **2010**, *3*, 193–199. [CrossRef]
15. McKay, K.; Bassham, L.; Sönmez Turan, M.; Mouha, N. *Report on Lightweight Cryptography*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
16. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [CrossRef]
17. Qiu, T.; Chen, N.; Li, K.; Atiquzzaman, M.; Zhao, W. How can heterogeneous internet of things build our future: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2011–2027. [CrossRef]
18. Al-Masri, E.; Kalyanam, K.R.; Batts, J.; Kim, J.; Singh, S.; Vo, T.; Yan, C. Investigating messaging protocols for the Internet of Things (IoT). *IEEE Access* **2020**, *8*, 94880–94911. [CrossRef]
19. Erdinc, O.; Vural, B.; Uzunoglu, M. A dynamic lithium-ion battery model considering the effects of temperature and capacity fading. In Proceedings of the 2009 International Conference on Clean Electrical Power 2009, Capri, Italy, 9–11 June 2009; IEEE: New York, NY, USA, 2009; pp. 383–386.
20. Azari, A.; Stefanović, Č.; Popovski, P.; Cavdar, C. On the Latency-Energy Performance of NB-IoT Systems in Providing Wide-Area IoT Connectivity. *IEEE Trans. Green Commun. Netw.* **2020**, *4*, 57–68. [CrossRef]
21. Al-Janabi, T.A.; Al-Raweshidy, H.S. An Energy Efficient Hybrid MAC Protocol With Dynamic Sleep-Based Scheduling for High Density IoT Networks. *IEEE Internet Things J.* **2019**, *6*, 2273–2287. [CrossRef]
22. Chulde, C.H.; Cantero, J.P. Internet of Things implementation with nodes based on low-power microcontroller MSP430. In Proceedings of the 2017 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 23–25 November 2017; IEEE: New York, NY, USA, 2017; pp. 33–40.

23. Sanislav, T.; Mois, G.D.; Zeadally, S.; Folea, S.C. Energy harvesting techniques for internet of things (IoT). *IEEE Access* **2021**, *9*, 39530–39549. [CrossRef]
24. Kaur, N.; Sood, S.K. An Energy-Efficient Architecture for the Internet of Things (IoT). *IEEE Syst. J.* **2017**, *11*, 796–805. [CrossRef]
25. Kim, N.; Austin, T.; Baauw, D.; Mudge, T.; Flautner, K.; Hu, J.; Irwin, M.; Kandemir, M.; Narayanan, V. Leakage current: Moore's law meets static power. *Computer* **2003**, *36*, 68–75. [CrossRef]
26. Jiang, H.; Marek-Sadowska, M.; Nassif, S. Benefits and costs of power-gating technique. In Proceedings of the 2005 International Conference on Computer Design, San Jose, CA, USA, 2–5 October 2005; IEEE: New York, NY, USA, 2005; pp. 559–566. [CrossRef]
27. Zhuo, C.; Luo, S.; Gan, H.; Hu, J.; Shi, Z. Noise-Aware DVFS for Efficient Transitions on Battery-Powered IoT Devices. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 1498–1510. [CrossRef]
28. Dunkels, A.; Gronvall, B.; Voigt, T. Contiki—A lightweight and flexible operating system for tiny networked sensors. In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, Tampa, FL, USA, 16–18 November 2004; IEEE: New York, NY, USA, 2004; pp. 455–462. [CrossRef]
29. Santana, T.V.; Galindo-Serrano, A.; Sayrac, B.; López, S.M. Dynamic network configuration: Hotspot identification for Virtual Small Cells. In Proceedings of the 2016 International Symposium on Wireless Communication Systems (ISWCS), Poznan, Poland, 20–23 September 2016; IEEE: New York, NY, USA, 2016; pp. 49–53. [CrossRef]
30. Gomez, C.; Oller, J.; Paradells, J. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors* **2012**, *12*, 11734–11753. [CrossRef]
31. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
32. Qiao, L.; Zheng, Z.; Cui, W.; Wang, L. A survey on WiFi HaLow technology for Internet of Things. In Proceedings of the 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 20–22 October 2018; IEEE: New York, NY, USA, 2018; pp. 1–5.
33. Adame, T.; Bel, A.; Bellalta, B.; Barcelo, J.; Oliver, M. IEEE 802.11AH: The WiFi approach for M2M communications. *IEEE Wirel. Commun.* **2014**, *21*, 144–152. [CrossRef]
34. Gambier, P.; Anton, S.; Kong, N.; Erturk, A.; Inman, D. Piezoelectric, solar and thermal energy harvesting for hybrid low-power generator systems with thin-film batteries. *Meas. Sci. Technol.* **2011**, *23*, 015101. [CrossRef]
35. Wu, J.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
36. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
37. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *J. Netw. Comput. Appl.* **2016**, *67*, 147–165. [CrossRef]
38. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
39. Sacramento, L.; Medeiros, I.; Bota, J.; Correia, M. Flowhacker: Detecting unknown network attacks in big traffic data using network flows. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing Additionally, Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: New York, NY, USA, 2018; pp. 567–572.
40. Groza, B.; Minea, M. Formal modelling and automatic detection of resource exhaustion attacks. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; Association for Computing Machinery: New York, NY, USA, 2011; pp. 326–333.
41. Mansfield-Devine, S. The evolution of DDoS. *Comput. Fraud Secur.* **2014**, *2014*, 15–20. [CrossRef]
42. Janes, B.; Crawford, H.; OConnor, T. Never ending story: Authentication and access control design flaws in shared IoT devices. In Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 21 May 2020; IEEE: New York, NY, USA, 2020; pp. 104–109.
43. Bagga, M.; Thakral, P.; Bagga, T. A Study on IoT: Model, Communication Protocols, Security Hazards & Countermeasures. In Proceedings of the 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 20–22 December 2018; IEEE: New York, NY, USA, 2018; pp. 591–598.
44. Bakhshi, T.; Ghita, B.; Kuzminykh, I. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors* **2024**, *24*, 708. [CrossRef] [PubMed]
45. Albalawi, A.; Almrshed, A.; Badhib, A.; Alshehri, S. A Survey on Authentication Techniques for the Internet of Things. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; IEEE: New York, NY, USA, 2019; pp. 1–5. [CrossRef]
46. Shivraj, V.; Rajan, M.; Singh, M.; Balamuralidhar, P. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In Proceedings of the 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 17–19 February 2015; IEEE: New York, NY, USA, 2015; pp. 1–6.
47. Sidhu, S.; Mohd, B.J.; Hayajneh, T. Hardware security in IoT devices with emphasis on hardware trojans. *J. Sens. Actuator Netw.* **2019**, *8*, 42. [CrossRef]
48. Mavrovouniotis, S.; Ganley, M. Hardware security modules. In *Secure Smart Embedded Devices, Platforms and Applications*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 383–405.

49. Raymundo Belleza, R.; de Freitas Pignaton, E. Performance study of real-time operating systems for internet of things devices. *IET Softw.* **2018**, *12*, 176–182. [CrossRef]
50. Liu, Y.; Briones, J.; Zhou, R.; Magotra, N. Study of secure boot with a FPGA-based IoT device. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; IEEE: New York, NY, USA, 2017; pp. 1053–1056.
51. Simon, T.; Batina, L.; Daemen, J.; Grosso, V.; Massolino, P.M.C.; Papagiannopoulos, K.; Regazzoni, F.; Samwel, N. Friet: An authenticated encryption scheme with built-in fault detection. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques 2020, Zagreb, Croatia, 10–14 May 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 581–611.
52. Zhao, S.; Zhang, Q.; Qin, Y.; Feng, W.; Feng, D. Sectee: A software-based approach to secure enclave architecture using tee. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1723–1740.
53. Arthur, W.; Challener, D.; Goldman, K. *A Practical Guide to TPM 2.0: Using the New Trusted Platform Module in the New Age of Security*; Springer Nature: Berlin, Germany, 2015.
54. Al Fardan, N.J.; Paterson, K.G. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; IEEE: New York, NY, USA, 2013; pp. 526–540. [CrossRef]
55. Freier, A.; Karlton, P.; Kocher, P. The Secure Sockets Layer (SSL) Protocol Version 3.0. Technical Report. 2011. Available online: https://www.rfc-editor.org/rfc/rfc6101.html (accessed on 1 March 2024).
56. Durumeric, Z.; Kasten, J.; Bailey, M.; Halderman, J.A. Analysis of the HTTPS certificate ecosystem. In Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, 23–25 October 2013; Association for Computing Machinery: New York, NY, USA, 2013; pp. 291–304.
57. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
58. Tian, Y.; Xu, K.; Ansari, N. TCP in wireless environments: Problems and solutions. *IEEE Commun. Mag.* **2005**, *43*, S27–S32. [CrossRef]
59. 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]
60. Shif, L.; Wang, F.; Lung, C.H. Improvement of security and scalability for IoT network using SD-VPN. In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; IEEE: New York, NY, USA, 2018; pp. 1–5. [CrossRef]
61. Butun, I.; Morgera, S.D.; Sankar, R. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 266–282. [CrossRef]
62. Liao, H.J.; Richard Lin, C.H.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. *J. Netw. Comput. Appl.* **2013**, *36*, 16–24. [CrossRef]
63. Bhatt, S.; Manadhata, P.K.; Zomlot, L. The Operational Role of Security Information and Event Management Systems. *IEEE Secur. Priv.* **2014**, *12*, 35–41. [CrossRef]
64. Samrin, R.; Vasumathi, D. Review on anomaly based network intrusion detection system. In Proceedings of the 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Mysuru, India, 15–16 December 2017; IEEE: New York, NY, USA, 2017; pp. 141–147. [CrossRef]
65. Frahim, J.; Santos, O.; Ossipov, A. *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*; Pearson Education: London, UK, 2014.
66. Kwon, S.; Choi, H.K. Evolution of WiFi Protected Access: Security Challenges. *IEEE Consum. Electron. Mag.* **2021**, *10*, 74–81. [CrossRef]
67. Meng, N.; Nagy, S.; Yao, D.; Zhuang, W.; Argoty, G.A. Secure coding practices in java: Challenges and vulnerabilities. In Proceedings of the 40th International Conference on Software Engineering, Gothenburg, Sweden, 27 May–3 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 372–383.
68. Hatzivasilis, G. Password-hashing status. *Cryptography 2017, 1*; Molecular Diversity Preservation International (MDPI): Basel, Switzerland, 2017; p. 10.
69. Smirnov, A.; Chiueh, T.C. Automatic patch generation for buffer overflow attacks. In Proceedings of the Third International Symposium on Information Assurance and Security, Manchester, UK, 29–31 August 2007; IEEE: New York, NY, USA, 2007; pp. 165–170.
70. Meneely, A.; Tejeda, A.C.R.; Spates, B.; Trudeau, S.; Neuberger, D.; Whitlock, K.; Ketant, C.; Davis, K. An empirical investigation of socio-technical code review metrics and security vulnerabilities. In Proceedings of the 6th International Workshop on Social Software Engineering, Hong Kong, China, 17 November 2014; Association for Computing Machinery: New York, NY, USA, 2014; pp. 37–44.
71. Fonseca, J.; Vieira, M. A survey on secure software development lifecycles. In *Software Development Techniques for Constructive Information Systems Design*; IGI Global: Hershey, PA, USA, 2013; pp. 57–73.

72. Schumacher, M. *Security Engineering with Patterns: Origins, Theoretical Models, and New Applications*; Springer Science & Business Media: Berlin, Germany, 2003; Volume 2754.
73. Schagen, N.; Koning, K.; Bos, H.; Giuffrida, C. Towards automated vulnerability scanning of network servers. In Proceedings of the 11th European Workshop on Systems Security, Porto, Portugal, 23–26 April 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–6.
74. Casey, E.; Stellatos, G.J. The impact of full disk encryption on digital forensics. *ACM SIGOPS Oper. Syst. Rev.* **2008**, *42*, 93–98. [CrossRef]
75. Shmueli, E.; Vaisenberg, R.; Gudes, E.; Elovici, Y. Implementing a database encryption solution, design and implementation issues. *Comput. Secur.* **2014**, *44*, 33–50. [CrossRef]
76. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of multi-factor authentication for securing advanced IoT applications. *IEEE Netw.* **2019**, *33*, 82–88. [CrossRef]
77. Siriwardena, P. *Advanced API Security*; Apress: New York, NY, USA, 2014.
78. Sidorov, V.; Ng, W.K. Transparent data encryption for data-in-use and data-at-rest in a cloud-based database-as-a-service solution. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015; IEEE: New York, NY, USA, 2015; pp. 221–228.
79. Ghouse, M.; Nene, M.J.; Vembuselvi, C. Data leakage prevention for data in transit using artificial intelligence and encryption techniques. In Proceedings of the 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 20–21 December 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
80. He, W.; Golla, M.; Padhi, R.; Ofek, J.; Dürmuth, M.; Fernandes, E.; Ur, B. Rethinking Access Control and Authentication for the Home Internet of Things ({{{{{IoT}}}}}). In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; USENIX Association: Berkeley, CA, USA, 2018; pp. 255–272.
81. Sandhu, R.S. Role-based access control. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 1998; Volume 46, pp. 237–286.
82. Mao, B.; Kawamoto, Y.; Liu, J.; Kato, N. Harvesting and threat aware security configuration strategy for IEEE 802.15. 4 based IoT networks. *IEEE Commun. Lett.* **2019**, *23*, 2130–2134. [CrossRef]
83. Xie, W.; Jiang, Y.; Tang, Y.; Ding, N.; Gao, Y. Vulnerability detection in iot firmware: A survey. In Proceedings of the 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, 15–17 December 2017; IEEE: New York, NY, USA, 2017; pp. 769–772.
84. Nilsson, D.K.; Larson, U.E. Secure firmware updates over the air in intelligent vehicles. In Proceedings of the ICC Workshops-2008 IEEE International Conference on Communications Workshops, Beijing, China, 19–23 May 2008; IEEE: New York, NY, USA, 2008; pp. 380–384.
85. Mugarza, I.; Flores, J.L.; Montero, J.L. Security issues and software updates management in the industrial internet of things (iiot) era. *Sensors* **2020**, *20*, 7160. [CrossRef]
86. Okhravi, H.; Nicol, D. Evaluation of patch management strategies. *Int. J. Comput. Intell. Theory Pract.* **2008**, *3*, 109–117.
87. Schlette, D.; Caselli, M.; Pernul, G. A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2525–2556. [CrossRef]
88. Shinde, N.; Kulkarni, P. Cyber incident response and planning: A flexible approach. *Comput. Fraud Secur.* **2021**, *2021*, 14–19. [CrossRef]
89. Neisse, R.; Steri, G.; Baldini, G. Enforcement of security policy rules for the internet of things. In Proceedings of the 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Larnaca, Cyprus, 8–10 October 2014; IEEE: New York, NY, USA, 2014; pp. 165–172.
90. Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A lightweight encryption algorithm for secure internet of things. *arXiv* **2017**, arXiv:1704.08688.
91. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
92. Ekanayake, V.; Kelly IV, C.; Manohar, R. An ultra low-power processor for sensor networks. In Proceedings of the 11th International Conference on Architectural Support for Programming Languages and Operating Systems, Boston, MA, USA, 7–13 October 2004; Association for Computing Machinery: New York, NY, USA, 2004; pp. 27–36.
93. Li, T.; Zhang, J.; Obaidat, M.S.; Lin, C.; Lin, Y.; Shen, Y.; Ma, J. Energy-efficient and secure communication toward UAV networks. *IEEE Internet Things J.* **2021**, *9*, 10061–10076. [CrossRef]
94. 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]
95. Potlapally, N.R.; Ravi, S.; Raghunathan, A.; Jha, N.K. A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE Trans. Mob. Comput.* **2005**, *5*, 128–143. [CrossRef]
96. Nawrocki, P.; Sniezynski, B.; Kolodziej, J.; Szynkiewicz, P. Adaptive context-aware energy optimization for services on mobile devices with use of machine learning considering security aspects. In Proceedings of the 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, VIC, Australia, 11–14 May 2020; IEEE: New York, NY, USA, 2020; pp. 708–717. [CrossRef]

97. Dini, P.; Elhanashi, A.; Begni, A.; Saponara, S.; Zheng, Q.; Gasmi, K. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. *Appl. Sci.* **2023**, *13*, 7507. [CrossRef]
98. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
99. Sultan, I.; Mir, B.J.; Banday, M.T. Analysis and Optimization of Advanced Encryption Standard for the Internet of Things. In Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 27–28 February 2020; IEEE: New York, NY, USA, 2020; pp. 571–575.
100. Ahtsham, M.; Yan, H.Y.; Ali, U. IoT based door lock surveillance system using cryptographic algorithms. In Proceedings of the 2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC), Banff, AB, Canada, 9–11 May 2019; IEEE: New York, NY, USA, 2019; pp. 448–453.
101. Hutchinson, S.; Stanković, M.; Ho, S.; Houshmand, S.; Karabiyik, U. Investigating the Privacy and Security of the SimpliSafe Security System on Android and iOS. *J. Cybersecur. Priv.* **2023**, *3*, 145–165. [CrossRef]
102. Chi, Q.; Yan, H.; Zhang, C.; Pang, Z.; Da Xu, L. A reconfigurable smart sensor interface for industrial WSN in IoT environment. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1417–1425.
103. Ramos, J.L.H.; Bernabe, J.B.; Skarmeta, A.F. Managing context information for adaptive security in IoT environments. In Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, Republic of Korea, 24–27 March 2015; IEEE: New York, NY, USA, 2015; pp. 676–681.
104. Ferrag, M.A.; Shu, L. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet Things J.* **2021**, *8*, 17236–17260. [CrossRef]
105. Bakhouyi, A.; Dehbi, R.; Talea, M.; Hajoui, O. Evolution of standardization and interoperability on E-learning systems: An overview. In Proceedings of the 2017 16th International Conference on Information Technology Based Higher Education and Training (ITHET), Ohrid, Macedonia, 10–12 July 2017; IEEE: New York, NY, USA, 2017; pp. 1–8. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.