electronics

Review

Security and Internet of Things: Benefits, Challenges, and Future Perspectives

Hamed Taherdoost [1,2]

[1] Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada; hamed.taherdoost@gmail.com or hamed@hamta.org
[2] Research and Development Department, Hamta Group | Hamta Business Corporation, Vancouver, BC V6E 1C9, Canada

Abstract: Due to the widespread use of the Internet of Things (IoT), organizations should concentrate their efforts on system security. Any vulnerability could lead to a system failure or cyberattack, which would have a large-scale impact. IoT security is a protection strategy and defense mechanism that protects against the possibility of cyberattacks that specifically target physically linked IoT devices. IoT security teams are currently dealing with growing difficulties, such as inventories, operations, diversity, ownership, data volume, threats, etc. This review examines research on security and IoT with a focus on the situation, applications, and issues of the present as well as the potential for the future. IoT network security has received greater attention from interdisciplinary and geographically scattered researchers in recent years. Data integrity, secrecy, authentication, and authorization should be guaranteed due to the large amount of data that flows across network devices. However, the area of IoT security still has a lot of room for growth.

Keywords: Internet of Things; security; data security; network security

check for updates

Citation: Taherdoost, H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics* **2023**, *12*, 1901. https://doi.org/10.3390/electronics12081901

Academic Editors: Tony Jan, Deepak Puthal, Anca Ralescu and Mukesh Prasad

Received: 7 March 2023
Revised: 11 April 2023
Accepted: 14 April 2023
Published: 18 April 2023

1. Introduction

The world has experienced some significant technical advancements in computer networking during the twenty-first century, which is known as the age of wireless communication and interconnectivity. Kevin Ashton first used the phrase “Internet of Things (IoT)” in 1999 [1]. IoT is a recent technology that enables the development of networks connecting various items, whether in the real world or the digital one [2]. IoT devices, which range in size from tiny wearables to massive machinery and are outfitted with actuators and sensors, can intelligently sense their environments and take action on their own [3,4].

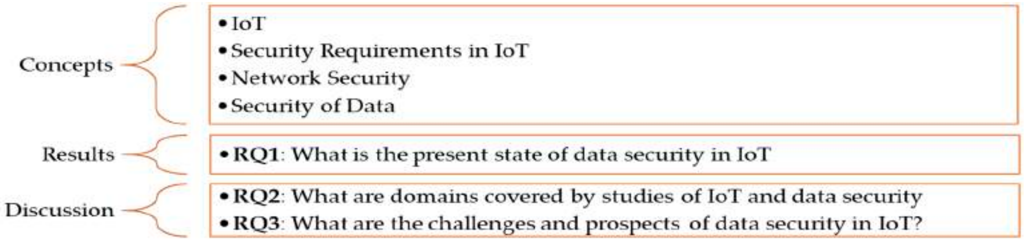
There will be an increase in the number of IoT applications and gadgets because more sectors are utilizing IoT apps. Wearable technology with devices to monitor and share a person’s behavior and health information is one such business that is providing wearable technology. IoT apps and gadgets are being made available to patients in the healthcare industry [5]. Currently available “smart house” IoT products include smart refrigerators, smart heating, smart gardening, video doorbells, personal assistants for smart lights, smart coffee makers, and smart door locks. Smart parking, smart street lights, and smart trash management are some of the “smart city” apps and IoT gadgets that have been developed [6].

IoT security has garnered a lot of interest in the scholarly community. The security of IoT devices has been a hot topic among academics [7–13]. IoT has many advantages, but it also has three main problems: data transmission, data gathering, and data security. Many tracking apps have been created specifically to collect data from IoT devices. IoT devices can connect to current networks and exchange data thanks to various protocols that have been developed and changed to transmit gathered data. However, they do not offer these protocols the attention they require. As a result, IoT is closely linked to many modern and traditional security problems, including identification, data security, permission, etc. Denial of service assaults, replay attacks, Denning-Sacco attacks, password guessing attacks, etc. can all result from login flaws. On the other hand, it is very difficult to authenticate IoT devices across heterogeneous and linked networks. These protocols should also consider problems with IoT device limitations, energy consumption, limited memory space, and limited computing power [14–19].

Mishra et al. [20] reviewed the development, uses, and difficulties of IoT. The security issues with IoT were highlighted using a layered perspective. To increase IoT security, anomalous detection methods were contrasted with the most current Intrusion Detection System (IDS). In the IoT, several kinds of assaults are mitigated by using authentication techniques and lightweight encryption algorithms, according to Hameed and Alomary [21]. The writers suggested that additional study is required to improve IoT gadget security. Using a four-layered cybersecurity-oriented design for IoT, Lu and Xu [22] addressed security assaults on IoT and showed a taxonomy of IoT cybersecurity attacks. They talked about its use in various sectors and assault defense strategies. Device security, transmission security, and data security were all included in the taxonomy of security criteria used by Harbi et al. [10] to evaluate IoT security. The report addressed the difficulties and suggested security solutions for several IoT uses.

A thorough analysis of the security-related difficulties and potential sources of threat in IoT apps was given by Hassija et al. [23]. The report offered thorough and practical suggestions for enhancing the IoT infrastructure to support secure interactions. In their final section, the authors covered how technologies such as machine learning, edge, cloud computing, and blockchain can be used to improve IoT security. Comparable issues with security and safety in IoT were covered by Jurcut et al. [24]. This is accomplished by emphasizing vulnerabilities that could result in a security breach as well as finding general threats and attack routes against IoT devices. This document also provided some security enhancements and prevention techniques to reduce risks, in addition to remedies for compromised devices. The security advantages that new technologies such as blockchain and software-defined networks (SDN) offer to IoT networks were addressed by Kouicem et al. [25]. Flexibility and scale are these two systems' primary security advantages. The study also examined the security needs and difficulties in various IoT apps. Security options can be divided into traditional and modern methods.

In the literature, earlier works [26–31] examined the security of IoT. The situation uses and concerns of data security within the framework of network security are the main emphasis of this study's examination of research on security and IoT. The purpose of this review is to handle the urgent issues depicted in Figure 1 through the following goals and research questions (RQs):



- IoT
- Security Requirements in IoT
- Network Security
- Security of Data

- **RQ1**: What is the present state of data security in IoT

- **RQ2**: What are domains covered by studies of IoT and data security
- **RQ3**: What are the challenges and prospects of data security in IoT?

Figure 1. The study's objectives.

The rest of this work is structured as follows. Section 2 discusses the study's context and advantages. Section 3 is dedicated to studying methods and paper selection. Section 4 summarizes the findings based on the current status of IoT and data security in the framework of network security. Section 5 discusses and compares selected works and examines the obstacles and opportunities. Lastly, Section 6 provides the conclusion.

2. Concepts

Several research papers and publications have investigated the security concerns and solutions of IoT [32–34]. To secure the security and confidentiality of IoT devices and networks, several fundamental concerns need to be addressed. Authenticating and authorizing devices to access networks and data is one of the most significant difficulties in safeguarding IoT [35]. This necessitates the deployment of robust encryption and authentication technologies, such as Public Key Infrastructure (PKI), to confirm the identification of devices and create secure communication channels [32]. The physical distribution of IoT devices makes them susceptible to physical assaults, such as tampering and theft. It is crucial to guarantee that these devices are protected from physical assaults by using tamper-resistant hardware and safe installation procedures [33]. This part of the paper covers a short introduction to IoT as well as contributions from the literature on IoT security requirements, network security, and data security.

2.1. IoT

A remotely controllable toaster that was first introduced in 1990 was the first basic gadget in this IoT category [36]. A Radio Frequency Identification-based system for item identification was the first widespread smart device application ten years later [37]. The variety of IoT smart applications has fully transformed the network world. Smart finance, smart grids, smart health care, and other smart services are examples of these uses [23]. Numerous applications of the IoT have revolutionized the industry. Predictive maintenance is one of the most important applications of the IoT in industry, where IoT sensors are used to monitor apparatus and machinery and determine when maintenance is required, thereby reducing downtime and increasing efficiency. IoT sensors can also be used to track assets such as products, containers, and vehicles in real-time, allowing for greater supply chain visibility and control. In addition, IoT sensors may be employed to monitor and optimize energy consumption, resulting in cost savings and a smaller carbon footprint. The technology is also suitable for the remote control and monitoring of industrial processes, tracking inventory levels, and automatically ordering supplies when stock is low. In addition to monitoring and detecting potential safety hazards, such as equipment malfunctions or gas leakage, IoT devices can also warn workers of potential dangers.

Numerous and diverse IoT applications in the industry offer significant advantages in the form of cost reductions, productivity, and efficiency. As the technology continues to develop, we can anticipate even more innovative IoT applications in the industry. It is important to note, however, that the implementation of the IoT in the industry comes with its own set of challenges, including the high cost of IoT infrastructure, data security and privacy concerns, and the requirement for specialized expertise and abilities for the development and maintenance of IoT systems. For industries to actualize the full potential of IoT, they need to evaluate the advantages and drawbacks of IoT implementation and work towards overcoming these obstacles.

Researchers have attempted to tackle these security issues using various methods [38]. Several additions have been made to the literature, but due to limited studies, one cannot obtain complete and varied views of security analysis. To close this gap, a thorough study and analysis are needed. The necessary analysis should not only emphasize problems but also explore potential solutions in a wider context.

2.2. Security Requirements in IoT

The security aspect of this technology is significant since recent surveys and trends have documented numerous developments in this area. This evolution of the assaulting mechanism has resulted in the development of numerous zero-day attacks [39]. Adversaries typically attempt to circumvent security frameworks by conducting zero-day attacks, which in turn slow down the network and greatly annoy legitimate users [40].

Information assurance can be defined as the practice of ensuring that information systems will function as expected when needed while remaining secure and protected.

Information assurance is defined as "measures that safeguard and preserve information and information systems by guaranteeing their secrecy, verification, integrity, availability, and non-repudiation", according to the National Institute of Standards and Technology [41]. These steps include "providing for the restoration of information networks by integrating security, detection, and response capabilities". Because IoT-based systems mix a digital information world with a physical equivalent, communication networks, and data resources, these five pillars of information assurance are relevant as security requirements [42].

IoT security requirements are crucial for ensuring the safe and secure operation of interconnected devices and the data they produce. Strong authentication and access control mechanisms to prevent unauthorized access and defend against cyberattacks are essential IoT security requirements. These mechanisms need to be capable of identifying and authenticating users and devices, controlling access to sensitive data, and providing granular permissions to ensure that only authorized entities can access the system. Moreover, data generated by IoT devices should be encrypted and protected to ensure privacy and confidentiality. Additionally, the data should be protected from tampering to ensure its integrity and authenticity. Network and device security is another vital aspect of IoT security. IoT devices and systems need to be protected from network-based assaults. Physical assaults, such as destruction, larceny, and tampering, should also be prevented by IoT devices' inbuilt security mechanisms.

2.3. Network Security

The IoT combines the physical and Internet-connected worlds to provide intelligent collaboration between physical entities and their surrounding environments. Typically, IoT devices work in a variety of environments to accomplish a variety of goals. Nonetheless, their business needs to adhere to stringent cybersecurity and physical security standards [43,44]. The participation of interdisciplinary components, networks, computations, and so on contributes to the composite character of IoT settings. This broadens the attack areas of IoT-based systems and makes meeting security restrictions more difficult. To meet the expected IoT security requirements, a solution with all-inclusive factors is required. Nonetheless, IoT devices are typically used in congested and open settings. As a result, attackers/intruders can directly reach IoT devices. IoT devices are usually linked across wireless communication networks, where attackers/intruders can impersonate eavesdropping to extract sensitive information from the communication. Because of their limited resources, IoT devices cannot support complex security solutions [45]. As a result, preserving the privacy or security of IoT-based devices is a multifaceted and difficult job that has sparked considerable interest in both scholarly and industrial areas. Given that the primary goal of an IoT-based system is to provide simple access to anyone, anywhere, and at any time, attack surfaces become more vulnerable to different attacks [46].

IoT devices generate vast quantities of data, which are transmitted over networks, making them susceptible to cyber threats. Consequently, securing the network and data in IoT is essential for the safety and security of the entire system. Network security measures provide the foundation for securing data in transit, whereas data security measures safeguard data in transit and at rest. To ensure the secure and safe operation of IoT devices and systems, it is necessary to employ a comprehensive security strategy that includes both network and data security measures.

2.4. Security of Data

Information assurance is a broad category of security standards or goals that only pertain to particular digital information systems. Because of this, this section goes into great detail about the goals and/or requirements of IoT security. The reasons why these requirements are challenging to meet about Industry 4.0 applications are also addressed, giving readers helpful insights into why the contentious security requirements are challenging to meet using conventional techniques. The requirements for an IoT-based device's security can be summed up as follows.

The digital world will now document data security as an essential security element, and the introduction of IoT will make data security an indispensable aspect of the creation of safe IoT systems. Several works [47–49] deemed data secrecy to be a security requirement for IoT data. Nonetheless, data consistency and data access are considered more beneficial than secrecy, particularly in industrial environments [50,51], because they have a measurable business impact. This is an unsuitable point of view in the context of a networked device world, with businesses quickly shifting their offline platforms to be internet-connected frameworks. According to company-based survey studies [52], it was found and proven that data protection is an important motivator for businesses to migrate to Industry 4.0 [49]. Furthermore, it was stated that businesses were hesitant to adopt data-sharing-based methods (such as cloud sharing, prevention, flaw detection, and so on) due to the lack of proof about the security or safety of these methods during the protection of intellectual property. As a result, this highlighted the need for a consistent strategy to safeguard the rational estate of the presence of data-sharing processes. In the early phases, there is widespread agreement that businesses are hesitant to rely on cloud servers for keeping and exchanging IoT data [53]. Nonetheless, the majority of IoT data violations are noticed within businesses rather than at cloud providers. Then, cloud-based storage was developed to reduce the surface of assaults on both the business and cloud sides. However, data loss mitigation has emerged as an additional requirement, identifying four critical processes required for creating an effective solution. Identification, prevention, recording, and notification are among these variables.

The difficulties in this area are linked with three interfering factors: To begin, due to the resource-constrained nature and mobility of IoT systems, data security methods need to operate in a manner that allows for very limited resource consumption. Second, numerous IoT facilities are supported by data sharing; however, in data-sensitive settings, secrecy is of utmost importance, which frequently presents numerous problems. Third, the need for data security increases dramatically, particularly in the case of sensitive IoT services or apps.

IoT security is a protection tactic and defense mechanism that guards against attacks that particularly target physically connected IoT devices. Network security protects the network and the data it contains from intrusions, assaults, and other threats. This is a wide and inclusive term that covers both software and hardware solutions as well as procedures, guidelines, and configurations for network use, accessibility, and threat avoidance in general. Encryption methods are just one aspect of the topic of data protection. Numerous benefits result from the combination of IoT and the Industry 4.0 paradigm, including better IoT data exploitation. This covers information sharing and other data-dependent operations that might take place anywhere in the system, even outside the organization's borders. While encryption methods enable preferential data exchange, this part elaborates on other strategies for maintaining the confidentiality of IoT data (Figure 2). Significant connections exist between the IoT and network security, cybersecurity, and data security. Protecting IoT devices and networks is vital for preventing cyberattacks. Network security protects the networks that link IoT devices. Cybersecurity requires defending the whole IoT ecosystem from cyber assaults, including devices, networks, and apps.

Data security is the safeguarding of data gathered and communicated by the IoT devices. This involves encrypting the data during transmission and storing it securely. In addition, access restrictions and authentication systems are crucial for preventing unwanted access to sensitive data. These data security measures are essential for protecting the data collected and transmitted by IoT devices [32]. IoT devices are susceptible to cyber threats, and protecting them entails installing network security, cybersecurity, and data protection safeguards.

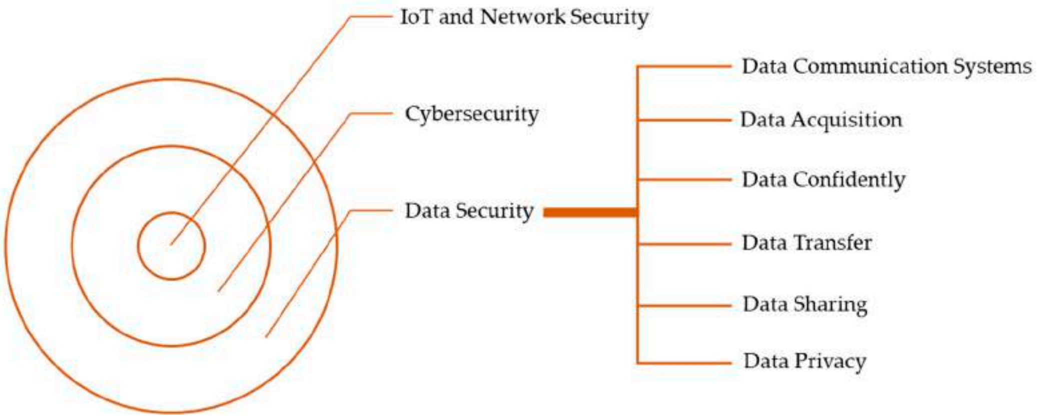


Figure 2. IoT info security: how important is it?

3. Research Method

Only when a literature review is founded on clear research questions, examines and analyzes other related research studies, and rates the quality of those studies using predetermined criteria can it be deemed a methodical literary study. This study adheres to the standards set forth by Kitchenham and Charters [54] and other systematic reviews [55,56] for performing systematic review studies. As a result, the definition of inclusion and exclusion criteria, data sources, and search methods are all separate phases of this systematic review. In the ensuing subsections, these phases are briefly addressed. Setting such criteria aims to guarantee that only studies pertinent to the research's purview are selected for further examination. This was accomplished by using the inclusion-exclusion standard to determine whether or not a particular piece should be chosen for study. The research papers chosen for this study's critical analysis need to adhere to the inclusion and rejection criteria listed in Table 1.

Table 1. Standards of inclusion and exclusion.

Inclusion Standards	Exclusion Standards
Should consider network security	Articles not written in English
Should include Data Privacy/Communication Systems/Transfer/Acquisition/Sharing/Confidently in the title/abstract/keywords	Duplicated articles
Document Type: Article	Articles in Press
Source Type: Journal	Articles not written between 2012 to 2022

Based on Scopus and Google Scholar, a systematic analysis was performed (1 March 2023). Finding the primary search terms that would serve as the foundation for this study was the first step in the search strategy. These were ("Internet of Things" AND "Network Security" OR ("Internet of Things" AND "Network" AND "Security") OR ("IoT" AND "Network Security") OR ("IoT" AND "Network" AND "Security"). It is crucial to choose the right terms at this point in the systematic review because they have an impact on the articles that are shortlisted for investigation. The aforementioned terms led to the retrieval of 564 documents. Duplication prevented the inclusion of 34 pieces. The overall number of articles decreased to 530 as a consequence. Based on the addition and exclusion criteria, each of these pieces is examined and filtered. As a result, 25 papers were used in the analysis because they satisfied the requirements. A flowchart of the complete review process, including the number of research papers excluded at each step, is shown in Figure 3.

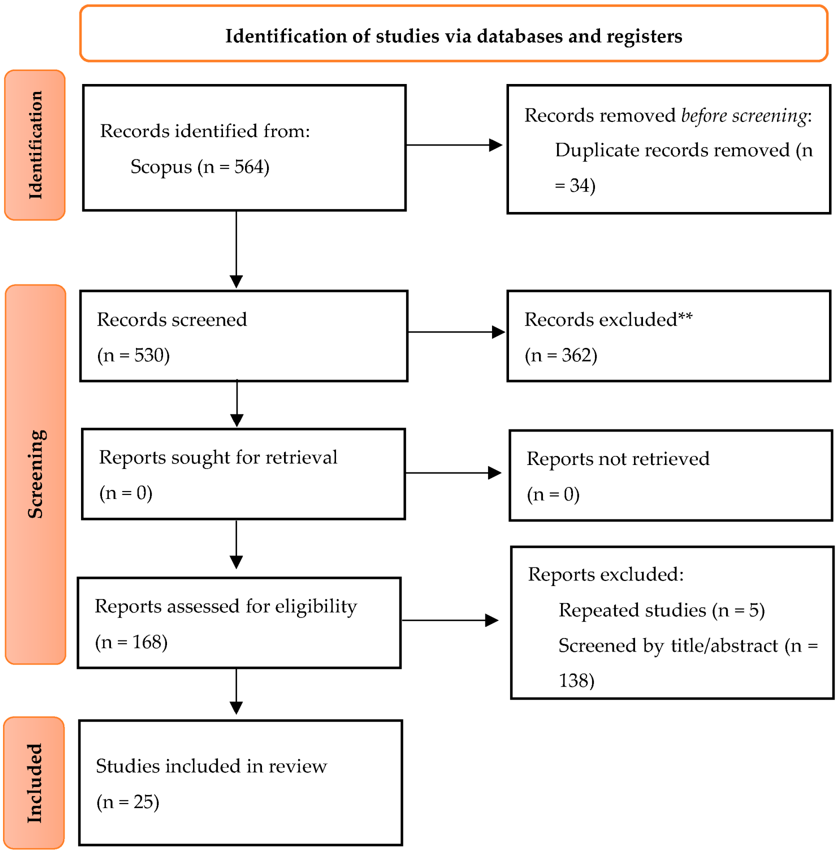

Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Scopus (n = 564)
Records removed *before screening*:
Duplicate records removed (n = 34)
Records screened
(n = 530)
Records excluded**
(n = 362)
Reports sought for retrieval
(n = 0)
Reports not retrieved
(n = 0)
Reports assessed for eligibility
(n = 168)
Reports excluded:
Repeated studies (n = 5)
Screened by title/abstract (n = 138)
Studies included in review
(n = 25)

Figure 3. Flowchart of the PRISMA literature search method. ** Number of papers excluded from the review according to the defined criteria.

4. Results

IoT software platforms are described as pieces of software that make it easier for IoT devices connected to a network to share data and services. A platform's characteristics [57] include data gathering, integration and storing, tracking, security, event processing, application enablement, processor analysis and visualization, device management, and connectivity and network management. The sanctity of data while in transmission, safe data storage, recognizing devices seeking a link and transmitting data, and permission of users or organizations are the four categories into which security solutions for a network can be broken down. The two types of IoT software platforms are cloud-based platforms and open-source platforms.

For many years, the IoT sector has fought back by developing IoT security tools that shield systems and devices from dangers and intrusions. Over the past few years, regulators and producers have begun to pay much greater attention to IoT gadget security. Figure 4 illustrates how the number of papers has grown over the previous ten years (2013: one article, 2017: one article, 2018: four articles, 2019: three articles, 2020: five articles, 2021: seven articles, and 2022: four articles). The security of IoT devices is anticipated to advance even further in 2023. While the route still faces obstacles, the adoption of new standards has strengthened best practices, and many of these adjustments will materialize in the coming year. This development is likely attributable to the rising deployment of IoT devices and systems across a variety of businesses, as well as a greater awareness of the security threats connected with these technologies. In recent years, there has been an increased emphasis on the security threats presented by IoT devices, such as the possibility of unauthorized access and control, data breaches, and privacy violations. In response, academics and industry professionals have been developing new security procedures, technologies, and best practices to solve these issues. The need to secure sensitive data, assure the availability and integrity of systems, and retain customer confidence in these technologies is the driving force behind the growing emphasis on security in the IoT arena. Thus, it is anticipated that the number of academic articles and business activities focusing on IoT security will continue to rise in the future years.

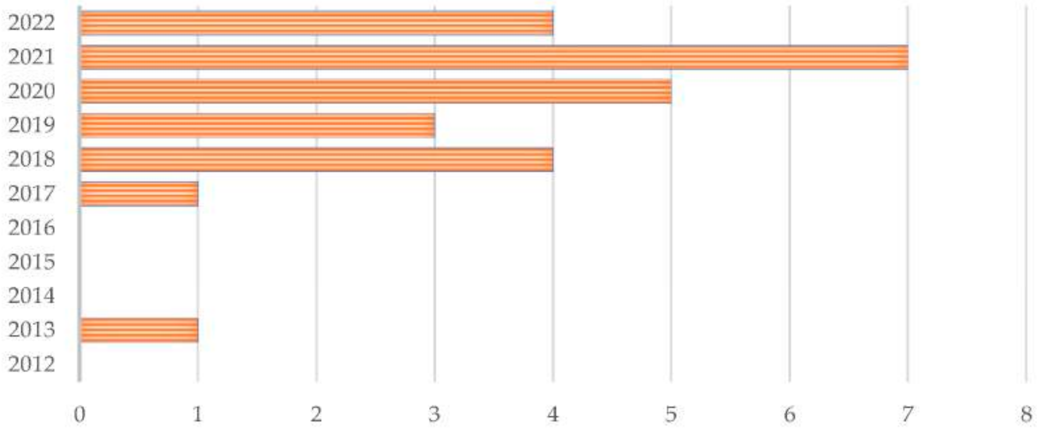


Figure 4. Number of articles.

The two journals with the most articles in the included research structure are IEEE *Internet of Things Journal* (three articles) and *Sensors Switzerland* (three articles). The following ones are *IEEE Access* (two articles), *Journal of Ambient Intelligence and Humanized Computing* (two articles), *Computers Materials and Continua* (one article), *IET Networks* (one article), *International Journal of Communication Systems* (one article), *International Journal of Distributed Sensor Networks* (one article), *International Journal of Safety and Security Engineering* (one article), *Journal of Information Security and Applications* (one article), *Journal of Parallel and Distributed Computing* (one article), *Mathematical Problems in Engineering* (one article), *Mobile Information Systems* (one article), *Neurocomputing* (one article), *Peer to Peer Networking and Applications* (one article), *Peerj Computer Science* (one article), *Web Intelligence* (one article), *Wireless Communications and Mobile Computing* (one article), and *Wireless Personal Communications* (one article). Figure 5 presents research distribution according to journals. Due to the growing relevance of security in IoT systems, several journals have prioritized the publication of articles on security and IoT. As IoT devices grow more pervasive and incorporated into critical infrastructure systems, it becomes more important to ensure their security. By publishing research on the most recent advances in IoT security, these journals contribute to the advancement of the state of the art in this field and enable policymakers, industry experts, and researchers to better understand the difficulties and possibilities associated with securing IoT systems.

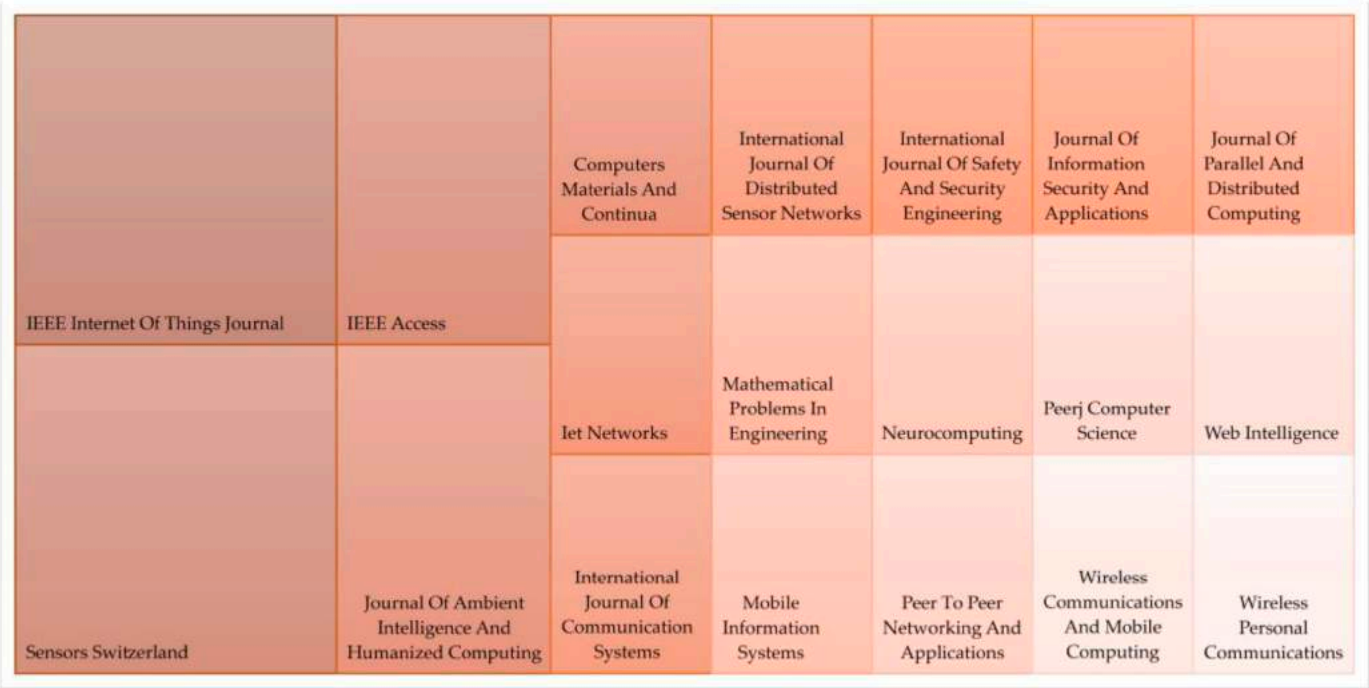


Figure 5. Research distribution according to Journals.

IoT study is typically found in papers that highlight applications in computer science and engineering. Similar to the IoT and Data Security topic categories, Computer Science (22 articles) and Engineering (13 articles) are obviously at the top of the list (Table 2). Some articles are common and interdisciplinary in different fields. In general, Computer Science and Engineering have concentrated on security and IoT articles because they play a crucial role in safeguarding IoT systems. As IoT devices become more pervasive and incorporated into critical infrastructure systems, the need for efficient security solutions will continue to increase, and computer science and engineering researchers will continue to play a crucial role in tackling these difficulties.

Table 2. Number of articles based on the subject area.

Subject Area	Number of Articles
Computer Science	22
Engineering	13
Mathematics	4
Biochemistry, Genetics and Molecular Biology	3
Chemistry	3
Materials Science	3
Physics and Astronomy	3
Decision Sciences	1
Environmental Science	1
Neuroscience	1

The two most common keywords used in articles are Internet of Things (24 articles) and Network Security (23 articles), which are the major terms of literature searches. The topics that will be covered include Authentication, Wireless Sensor Networks, and Data Security. Generally, terms such as "Internet of Things" and "Network Security" have been very significant to security and IoT studies, since they represent crucial parts of safeguarding IoT systems. By concentrating on these keywords, researchers may create new solutions and technologies to safeguard IoT devices and data from cyberattacks and guarantee their security and privacy. Figure 6 illustrates the distribution of keywords.

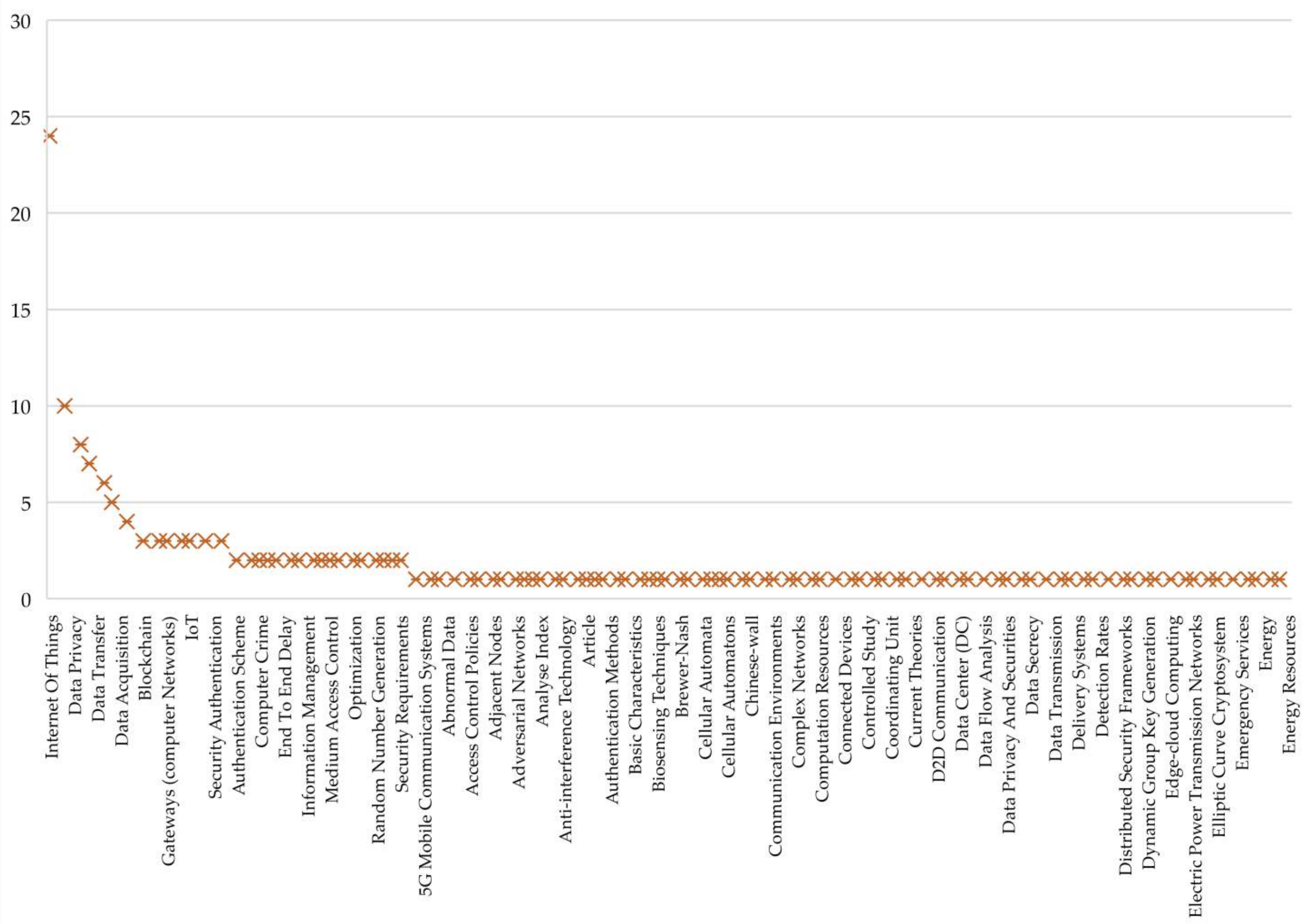


Figure 6. Distribution of keywords.

5. Discussion

A network is created when gadgets are interconnected to carry out specific duties. Both conventional and cellular networks are possible. People can benefit from useful knowledge that is shared or distributed through the network. Utilizing the network is essential for data to be transmitted more quickly. Information security refers to an organization's desire to protect information while it is being transmitted over a network. The confidentiality of data, data veracity, and data exposure to the appropriate individual are the three goals of information security [58].

Data security in the IoT or the cloud is a more recent area of computer security study that can benefit from the established findings in the more established field of data flow management for security [59]. Logrippo [59] approached the issue from a basic standpoint. They demonstrated that, under the assumptions of transitivity and reflexivity, any network of communicating entities can be viewed as a partial order of equivalence classes of entities. This generalized and simplified the current theory, which is based on the lattice concept and generates lattices through labeling. There are many methods to build networks of interacting entities, including routing, access control rules (which may involve naming), etc. For data security, their inherent partial orders were adequate and essential, and in any such network, entities will have varying levels of secrecy or integrity depending on where they are in the partial order. It was demonstrated how labeling systems—which can convey various security requirements—can be built to place things in the proper places within network partial orders. Examples were used to present well-established data security concepts such as disputes, conglomeration, and consolidation. The addition, deletion, or relocation of entities in partial orders as a consequence of occurrences such as user or managerial action was then demonstrated. The preservation of security needs through such transformations was explained using a label-based approach.

Many security-related problems with the current communication technologies need to be resolved to provide safe end-to-end connectivity among services. Additionally, the majority of common security methods that are currently thought to be safe may soon be in danger due to the recent, rapid development of quantum technologies. As a result, for contemporary security systems to withstand various possible quantum computer attacks, quantum technologies need to also be powerful. Quantum walks (QW) are regarded as a global quantum computation model and a top-notch key generator due to their unique properties [60]. In this respect, a novel, lightweight picture encryption method based on QW is suggested in the article by El-Latif et al. [60] for safe data transmission in IoT systems and wireless networking with edge computing. The newly proposed method builds permutation boxes using the power of QW's nonlinear dynamic behavior and creates pseudo-random numbers to encrypt the plain picture after splitting it into blocks. The outcomes of the performed modeling and numerical studies demonstrate the viability of the proposed encryption method. Because of the randomness of the encrypted pictures, it is impossible to decipher them by looking at the connection between neighboring pixels. Additionally, the entropy value is close to 8, the percentage of pixels that change is higher than 99.61 percent, and the key parameters are highly sensitive with a big key area to withstand different assaults. The article by Li et al. [61] developed a data security monitoring method based on narrow-band IoT to address the issues of bad data categorization accuracy and efficacy of conventional data monitoring methods. To begin collecting data for the intranet, a model of network data collection and the best setup for a sensor node were created. Dynamic intranet data analysis indexes were created from three perspectives based on the analysis of data characteristics: creating a security event quantity index, establishing an address entropy index, and data diversion. The security indicator of the IoT was computed by the narrow-band data aggregation rate previously stated to achieve the security of monitoring data. The testing findings demonstrated that, regardless of whether a network assault is present or not, the technique consistently accomplishes its design objectives in terms of accuracy rate (more than 90%), classification time (less than 4 s), and energy usage (less than 150 J).

IoT frequently offers the data gathering, administration, and device and data protection services needed for application development. IoT things or gadgets interact and compute to improve the comfort and security of our lives. IoT can be used for inventory automation, real-time item monitoring, and the administration of things' information and state. The vast quantity of data that moves between the devices in the network necessitates the creation of a security structure that guarantees the integrity, secrecy, authentication, and permission of data [62]. The sections that follow cover a few data protection solutions.

5.1. Authentication

In addition to its inherent limitations such as processing power, storage capacity, and energy resources, the proliferation of IoT devices is raising security vulnerabilities throughout the business. IoT security is becoming a bigger task for security experts to fight attack susceptibility. Given various security flaws, mobile IoT devices require a data routing mechanism to transmit the collected data [63]. The enormous rise in IoT usage has changed daily life in many countries, affecting the entire globe. IoT-based networks require protection just like any other program does because the data they generate contain sensitive data. The security methods currently used in these networks do not consider all security goals. The data need to be protected from different kinds of attacks as soon as they are sensed from the IoT world. Additionally, it needs to be possible to accomplish data integrity, access control, secrecy, and authentication of all concerned parties [64].

IoT's core features, such as its multi-hop autonomous design, frequent topology changes brought on by mobile IoT devices, shorter link life, media access latency, and multilayer security risks, make security-conscious routing an ongoing subject of discussion. To improve network efficiency through the best routing choice, cross-layer routing is also necessary. It uses dependency factors between protocol levels as routing parameters [63]. Kalyani and Chaudhari [63] presented a design for a secured cross-layer protocol that makes use of routing parameters calculated using the data shared from the Media Access Control layer. The Self Improved SLnO (SI-SLnO) method takes into account various limitations, such as "distance, energy, and risk factor of the route", when making routing decisions. For each ideal route, the risk component was calculated. Elliptic Curve Cryptography and Elgamal cryptosystem were used to determine the degree of data privacy needs using threshold-based risk factor utilization. Lastly, various metrics were used to verify the suggested secured cross-layer protocol's supremacy.

IoT device energy and computation resources are usually constrained, which makes studies into communication security and hacking in such networks challenging. Energy waste needs to be reduced because powerful security systems consume a lot of power. It is standard practice to use optimized application-specific security protocols to speed up data transmission while maintaining a high degree of security. The optimization should not have an impact on the enabled security features, such as secrecy, integrity, or validity [65]. The Host Identification Protocol is one of the current security protocols that Kaňuch and Macko [65] were working to optimize for use in the host identity protocol (HIP). They have found numerous opportunities for improvement and merged some of them into the suggested E-HIP optimized procedure based on an analysis of related studies. It has been modified and applied to a connection between actual hardware devices as a change of the open-source OpenHIP module for testing purposes. The encrypted transmission was successful. Experimental evaluation has determined that the suggested optimization's outcome is a rise in energy efficiency of about 20%. Although the suggested optimizations are distinctive and can be further integrated with some of the current ones to achieve even higher efficiency, the obtained results are comparable to those of other HIP optimizations.

To accomplish the authentication, Parne et al. [66] suggested several group-based authentications and key agreement (AKA) methods in the literature. All security criteria, including the protection of privacy, reciprocal authentication, integrity, and secrecy, are met by these procedures. However, none of them possesses the qualifications needed to solve the information network's one major issue. They are also vulnerable to recognized attacks and lack the effectiveness to keep the group key Unlink-Ability. Some protocols require each machine-type communication device to separately identify to access the communication network at the same time, which causes network congestion overhead. They suggest the security-enhanced group-based (SEGB) AKA algorithm for machine-to-machine transmission in an IoT-enabled LTE/LTE-A network in light of these issues. The SEGB-AKA protocol accomplishes key forward/backward confidentiality and resolves the issue of the single key during the authentication procedure. The algorithm solves the issue of excessive bandwidth usage and communication congestion. The automated Internet security procedures and apps' utility perform a formal security study of the protocol. The security study demonstrates that the protocol meets the security objectives and is immune to several well-known threats. In addition, the effectiveness of the suggested SEGB-AKA protocol is evaluated in comparison to the current group-based AKA protocols. The study demonstrates that the protocol performs better in terms of network overhead and satisfies all criteria for machine-to-machine communication security.

Tao et al. [67] introduced AccessAuth, a simple protocol for capacity-based security access verification. The optimal number of admissible access requests was first determined adaptively for each V2G network domain to effectively accomplish capacity-based access admittance control while taking into account the overload likelihood, system capacity limitations, and mobility of electric cars. Then, to implement strict access authentication and ensure that the sessions were only carried out by authorized requesters, a high-level authentication model with particular authentication protocols was provided. This was done to provide mutual authentication and maintain the data privacy of admitted sessions by examining whether there was previous knowledge of the trust connection between the relevant V2G network domains. Also covered were effective session termination with forward security and session recovery without an additional verification delay. Finally, analytical and assessment findings were given to show how well AccessAuth performs.

The ubiquitous IoT includes standards, programs, and tools for delivering uniform data. The method can be used to create an extensive data database that will help people evaluate, arrange, and use the data more effectively. This will increase the data's reliability and sharing, which will lead to improved services for users [68]. The goal of the study by Pan et al. [68] was to suggest and set up a particular, dependable data exchange program to guarantee the security of data exchange. The purpose of data security is to guarantee the validity of a particular security-sharing procedure. The dependability analysis method and the trade process behavior proof method are the main focus of their research. Based on the analysis of all abnormal phenomena in IoT traffic, the fundamentals of network traffic, the theory of multi-terminal power communication network anti-interference model construction, and the noninterference model, the simulation experiment of the anti-interference and security authentication method is carried out. The findings demonstrated that as the number of antennas is increased, the likelihood of erroneous detection drops from 10^{-1} to 10^{-4}, improving efficiency in the identification of active users. The most popular utility for data verification and security authentication when a network was involved was HTTP Plus SSL. The anti-interference technology industry has expanded quickly. The global market's complicated annual growth rate has nearly doubled, and the market's size has greatly increased with a yearly expansion rate of about 50%.

By offering autonomous support for operations and communications, the IoT plays a crucial part in the real world by allowing and supporting cutting-edge services that are frequently used in daily life. To defend against different assaults on IoT networks, it is crucial to conduct a study on security protocols for next-generation IoT and create cutting-edge confidentiality protection schemes [69]. The blockchain emerges as a viable option to provide notable features such as constant secrecy, authentication, and robustness. Medhane et al. [69] showed an SDN and edge cloud-based distributed security architecture that supports blockchain. The IoT network's edge layer experiences a reduction in security assaults as a result of the security attack monitoring being accomplished at the cloud layer. The SDN-enabled gateway provided dynamic network traffic flow management, which helped identify security attacks by identifying suspicious network traffic flows and reduced security assaults by obstructing suspicious flows. The outcomes demonstrated that the suggested security framework can successfully address the problems with data secrecy brought on by the merger of the SDN paradigm, edge cloud, and blockchain.

A study hotspot in the IoT business is how to satisfy the urgent needs of present consumers for trusted transmission services given the IoT technology's rapid growth in the information society. On networks built on the IoT, securing data exchange and transmission has always been difficult [70]. The article by Zhang and Xu [70] proposed a security authentication technique based on a dynamic Bayesian network coupled with a trustworthy protocol in light of the state of the research on security authentication in the IoT. The trusted measurement and integrated public key-based security verification method have been brought into the network to help users of the IoT choose a highly secure and dependable route for data transfer. This enhanced the security information sharing and improved routing choices by considering node credibility and path dependability. The evaluation's findings demonstrated that, for real-time apps, their algorithm outperforms comparative algorithms in terms of overhead and computational complexity. Their algorithm also had an adaptive capacity and can respond rapidly to a denial-of-service assault, successfully squelching the danger of abnormal IoT entities. Peer-to-peer (P2P) networks with blockchain support made an appropriate infrastructure for IoT and Beyond 5G apps. The network's distributed architecture and security services allowed for a wider range of financial activities, which is a benefit. Diverse IoT devices, security concerns, and energy-related problems are just a few of the problems with IoT-based networks [71]. Sankar et al. [71] described how to apply data security using a secured authentication technique, public blockchain for peer-to-peer transmission, and private blockchain for SDN. They incorporated an extra component where the sender signs the specific action while transferring the data from one user to another user to improve secrecy and non-repudiation. Public-key value-based signatures created with the transaction's private key are released along with it. Nodes verified this action using the created public key value-based signature. Better immutability is provided by the hashing procedure in encryption. When compared to the current techniques, the findings showed better speed and reaction time and a decrease in end-to-end latency and overhead, while also demonstrating increased security during data transfer. The Ethereum platform's Pyethereum testing utility was used in this project.

A novel security design was put forth by Ali and Mathew [64] for distributed IoT apps. The most popular lightweight encryption in the design is ChaCha20. To increase security and unpredictability, random number creation is performed using cellular automata principles. Data were protected on multiple levels during the posting and saving processes thanks to double encryption. The security of the technique was ensured by using dynamic session passwords for encryption. Additionally, it guaranteed message integrity, quick execution, user verification, and safe data exchange between communicating organizations. The IoT device linked to the gateway server needs to finish the registration step effectively. The mutual authentication step is then carried out each time a data transmission between the device and gateway server occurs. The use of a blockchain network at the periphery level guarantees participant node authentication, preventing accidental data change. Regarding throughput, execution time, and resilience to different security threats, the suggested design showed itself to be effective.

5.2. Wireless Networks

Wireless sensing networks are a key component of the IoT and have found widespread application in all facets of people's lives. In wireless sensor networks, identity verification ensures users' access to real-time data from sensor nodes without risk [72]. Many tiny devices are used in an IoT-based wireless sensor network (WSN) to gather data and transmit them to central archives. These battery-powered, resource-constrained sensors spend the majority of their energy detecting, gathering, and transmitting data. Security is a major worry in these networks when exchanging data because they are vulnerable to numerous threats, the bloodiest of which is the wormhole assault. These attacks are initiated without obtaining crucial network information, and they seriously jeopardize the network's efficiency, security, and communication. The limited resource availability in the sensing devices makes its prevention more difficult in an IoT-based network context [73]. The ESWI method was created by Shahid et al. [73] to enhance efficiency and security while detecting wormhole attacks. To reduce overhead and energy consumption during operation, this method has been intended to be straightforward and less complex. Their method's simulation findings demonstrated comparable detection rates and packet transport ratios. Additionally, it resulted in significantly reduced energy usage, a decreased end-to-end delay, and improved output.

A crucial element of the IoT, wireless sensor networks have many applications in all areas of peoples' lives. Identity authentication guarantees users' risk-free access to real-time data from sensor nodes in wireless sensor networks [72]. An IoT-based WSN is used to collect data and send it to centralized storage. The majority of the energy used by these battery-operated, resource-constrained devices goes into data detection, collection, and transmission. As these networks exchange data, security is a top concern because they are susceptible to a variety of dangers, the deadliest of which is tunnel attack [73].

Wireless local area network (WLAN) technologies for the IoT are subject to severe security risks despite unprecedented developments because of their limited computational and memory resources, which restricts the use of robust intrusion prevention and security procedures. Security managers (sec-admins) need to regularly and thoroughly evaluate IoT devices for vulnerabilities to solve this issue. The first stage is an Internet-wide port search (IWPS). However, in the case of conventional port-scan traffic, the medium access control mechanism of IEEE 802.11ah, which was created especially for heterogeneous IoT traffic and low-power processes, can impair network performance. To guarantee data secrecy, stability, and availability, IPv6-enabled IoT devices need to also support the Internet security (IPSec) protocol. Although a port check aims to increase IoT security, the subsequent network speed may hurt IPSec services. They enhance IoT security over IEEE 802.11ah WLAN by optimizing IWPS [74]. Verma et al. [74] proposed novel mathematical models to evaluate IoT security, which deduced an optimal scan rate for sec-admins, based on IPsec services and port-scan network performance. The effectiveness of the proposed framework was demonstrated through a thorough numerical analysis, which also shows how their approach decreased risk to IoT devices while investigating them at the optimal scan rate.

Existing security programs such as SIMON or SPECK provide simple security measures but are susceptible to differential attacks due to their ease of use. Furthermore, built-in verification is not a feature of the available options [62]. Therefore, using WSN technology, the study by Batra et al. [62] provided a safe and compact IoT-based framework. Using the COOJA simulator, the suggested security strategy was contrasted to the already-available security systems SPECK and SIMON. The suggested method outperformed others by 2% fewer CPU cycles, 10% less execution time, 4% fewer memory needs, and at least a 10% greater security effect.

Using the formal proof tool ProVerif, Hu et al. [72] suggested a two-factor authentication system based on an elliptic curve cryptosystem and demonstrated its security. Their scheme offered a better degree of security than comparable schemes while still achieving adequate computational cost efficiency. A novel verification method that is also for WSNs was presented by Wu et al. [75]. The formal proof was then demonstrated using the random oracle model, and the formal verification procedure was listed using the protocol analysis tool ProVerif. The suggested scheme solved common issues and was compatible with IoT security properties when compared to some new schemes in terms of WSN security properties.

In the setting of the IoT, Yu et al. [76] suggested a method for WSNs that they call Data Authentication and En-route Filtering (DAEF). In the DAEF, an effective ID-based signature algorithm and provable secret-sharing encryption were used to create and disseminate signature shares. According to their security analysis, DAEF was capable of defending against both node compromise and denial of service assaults that involved the disruption of reports and selective sending. To demonstrate the benefits of DAEF over other similar schemes, they also evaluated energy usage. The devices in the WSN at the data center (DC) in the Energy IoT (EIoT) were vulnerable to attacks and were easily affected by issues with information security management (ISM), such as bad real-time performance and high complexity. Xie et al. [77] explained the DC WSN's structure for the EIoT, simulated the WSN using low-energy adaptive clustering hierarchy (LEACH), and forecasted various attack kinds. A real-time and dynamic ISM strategy for the WSN was created using this information. The framework and processes of LEACH were optimized in this design, and information fusion was used to lessen the amount of data transfer. The suggested plan, according to a simulation experiment, protected communication between neighboring nodes and between upper and lower levels, guaranteed the longevity of network security through real-time key updates, and fostered data transfer efficiency through information fusion.

Using an established identification cryptosystem, Sun et al. [78] investigated the flow of key backup, key storage, key update, verification key distribution, key distribution, key creation, key management, and key validity time settings for mobile IoT. The design technique of key management and authentication was enhanced using encryption. Storage starts at 32 bytes and increases to 84 bytes in registration stage 1, 82 bytes in registration stage 2, and 356 bytes in authentication stage 3, after the number of bytes increases during the logon authentication stage. This procedure had some benefits for assuring safety performance. In their research on secure beamforming for a two-way cognitive radio (CR)

IoT network, Deng et al. [79] considered the benefits of concurrent wireless data and power transmission (SWIPT). The IoT manager, which was at the heart of the secondary network, used the primary spectrum to send data and power to the other IoT devices while assisting two primary users (PUs) with relay assistance and joint physical layer security against an eavesdropper. By collaboratively designing the beamforming matrix and vectors at the central controller, they sought to optimize the secrecy sum rate (SSR) for PUs to improve information security. They first suggested the branch-reduce-and-bound-based method to effectively solve the nonconvex problem by obtaining an upper limit for the SSR and providing a workable solution by Gaussian randomization, which required two levels of iteration and was therefore very complicated. They then suggested an iterative algorithm based on constrained-convex-concave programming and a non-iterative algorithm based on zero forcing, the latter of which had the lowest complexity and was suitable for the central controller with limited power supply, to strike a balance between performance and complexity. The simulation findings were given to show how well their suggested optimization techniques compare to the established methods.

5.3. Use Cases

In network engineering, today's Industrial IoT (IIoT) is very sophisticated, and networks experience annual data leaks. To improve IIoT security defense under privacy regulations, an anti-intrusion monitoring device has been developed. High standards need to be met by the IoT's structural system and security performance parameters are required in an unfriendly network. The network system should employ a technique with a very low rate of data loss and high levels of stability [80]. Teng [80] adopted the first deep-learning network technology after evaluating numerous network designs. The LeNet-5 network was upgraded and optimized by the Convolutional Neural Network technology, and a new LeNet-7 was created. An IIoT anti-intrusion monitoring system was built by combining three network technologies. The system's effectiveness was evaluated and confirmed. The algorithm had a high detection rate, a low false-positive rate, and high data precision. To achieve the highest performance, the model's generality on high-performance data was verified and contrasted with privacy-aware task offloading techniques. As a result, the technology can be used to safeguard IIoT data privacy under the legislation.

The delivery method in the hospital information setting is evolving in the IoT era due to connected devices. Along with hopeful technical, economic, and societal prospects, the incorporation of IoT in healthcare has significant potential to enhance the effectiveness, safety, and quality of healthcare. However, there are security dangers associated with this integration, such as the possibility of a data leak brought on by malware that steals login credentials. Additionally, because the prospective devices are online-connected, the sensitive patient data may be exposed if they are hacked. Due to the pervasiveness of IoT entities in general and IoT-based healthcare specifically, security has thus become a crucial component of today's technological world [81]. A study on the method for anonymizing private health data shared in the IoT environment using a wireless communication system has been provided in the article by Yin et al. [81]. The algorithm specified records that cannot be disclosed by protecting user privacy to maintain security and privacy while users are engaging online. Additionally, the suggested method incorporated a safe encryption technique that permitted privacy for health data. In addition, they have offered an evaluation of the anonymity function of the method using algebraic functions. The findings demonstrated that the anonymization method ensures security features for the IoT system under consideration when used in the context of hospital communication systems.

In the home area network (HAN), sensors with IoT support offer safe transmission and data integrity. Sensors and the smart grid's energy readings and information exchange offer a fresh viewpoint on energy management [82]. The focus of Manimuthu and Ramesh's [82] work was on the secured data movement in HAN and ensuring client data privacy during crucial and urgent operations. Data were made readily accessible in real-time with the least amount of transmission delay. Gadgets were continually checked for life-saving and urgent services. The IoT-based machine-to-machine data transfer and packet delivery are the main topics of this article. It assisted in providing real-time access to user power usage data in tailored electronic devices as well as over the cloud. The prerequisites for creating a cost-effective IoT-HAN connected to a smart grid for energy-aware routing were demonstrated by this study effort. By placing sensors and a control gateway within a clearly defined boundary, the advanced design plan served to save energy during data processing and data transmission. Using both simulated and real data from sensors and concentrators, the data flow pattern and packet delivery rate were evaluated. MATLAB and a network simulator were used to assess the findings and flow patterns that were acquired. The created IoT-HAN arrangement was extremely beneficial for safe data transfer between various linked devices inside HAN. Future Spaces, an end-to-end hardware-software prototype offering fine-grained control over IoT connectivity to allow simple and safe administration of smart homes, was presented by Boussard et al. [83]. They accomplished enhanced networking security and automation by defining discrete, usage-oriented segments that rely on Software-Defined Networking-enabled home routers and the virtualization of network functions in the cloud. Users' ability to find, manage, and exchange connected assets across multiple domains while easily adjusting to different utilization settings was disrupted by this.

5.4. Challenges and Prospects

The digital planet can be controlled and monitored thanks to the IoT. The most recent technology to monitor the necessary data is the IoT. IoT is the answer to lowering intricacy and improving system efficiency in transportation, healthcare, and cyber systems. Pervasive computing enables the IoT to handle data and present the necessary graphical user interface. Information can be accessed through a computer system called cloud computing anywhere and anytime on the globe [58]. Table 3 groups several studies based on the data security environment. The majority of the featured papers are focused on data privacy. A few papers have discussed data sharing and data confidently. They may present open issues for IoT data security studies in the future.

Table 3. Classification of various research based on the context of data security.

	Data Privacy	Data Sharing	Data Communication Systems	Data Confidently	Data Acquisition	Data Transfer
Hu et al. [72]	√					
Kalyani and Chaudhari [63]	√					
Teng [80]	√					
Pan et al. [68]	√	√				
Yin et al. [81]	√					
Manimuthu and Ramesh [82]	√					√
Boussard et al. [83]	√					
Tao et al. [67]	√					
Parne et al. [66]	√					
Wu et al. [75]	√					
Shahid et al. [73]		√			√	
Ali and Mathew [64]						√
Sankar et al. [71]		√	√			√
Sun et al. [78]			√			
Zhang and Xu [70]			√			
Deng et al. [79]			√			
Verma et al. [74]				√		
Logrippo [59]				√		
Medhane et al. [69]				√		
Li et al. [61]					√	
Batra et al. [62]					√	
Yu et al. [76]					√	
Xie et al. [77]						√
El-Latif et al. [60]						√
Kaňuch and Macko [65]						√

There is still much room for improvement in the field of IoT security. Researchers need to be concerned in the area because there are numerous ongoing studies and difficulties. Here are a few current issues with IoT security [84]:

- The development of sufficient intelligent systems engineering through the application of some intelligent algorithms and machine learning is necessary for real-time data analysis and effective hardware design.
- Blockchain is severely limited when there are many servers. Some highly efficient methods can replace nodes, and using numerous resources can emerge as a popular way to address the problem.
- Using machine learning and refining methods such as artificial intelligence (AI) and deep learning to improve fog levels.
- The only goal of fog sharing is to protect fog-cloud processing. It may be a hopeful answer if realized.
- End-to-end encryption methods and sufficient shielding procedures are still required for gateways between various locations.
- To comprehend adversary assaults, edge devices need to be extremely safe and intelligent.

The rapid expansion of IoT adoption across many industries brings security concerns to the fore. IoT is still in its early stages due to the enormous amount of research that has been conducted in recent years. The security zone is the main cause of the several challenges IoT is experiencing that restrict its expansion. Smart systems can deal with a range of problems faced by the industrial sector, despite some integration challenges with IoT and wireless sensors in Industry 4.0. The development of IoT and wireless sensor technology has led to greater concerns about security, privacy, and data management. Businesses and manufacturers find it difficult to effectively manage the expanding volume of data being created. Big Data management and enhancing the intelligence of systems and devices both require AI algorithms. The algorithms are used to process the data throughout a range of time frames [85].

Manufacturers of IoT devices will progressively create and integrate security measures into their products. The growing consumer and business knowledge of IoT security breaches and exposure, government and industry labeling and certification initiatives, and the public relations and reputation expenses of handling breaches are important factors influencing this growth.

6. Conclusions

Businesses should focus their efforts on system security because the IoT is so widely used. Any flaw could lead to a system failure or cyberattack, which would then have a large-scale impact. IoT security is a protection strategy and defense mechanism that protects against the possibility of cyberattacks that specifically target physically linked IoT devices. Current challenges facing IoT security teams include inventories, operations, variety, management, data traffic, threats, etc. With an emphasis on the circumstances, uses, and problems of data security in the context of network security, this study analyzes studies on security and IoT.

By using the aforementioned keywords, 564 items were found. Duplication prevented the inclusion of 34 pieces. The overall number of articles decreased to 530 as a consequence. Based on the addition and exclusion criteria, each of these pieces is examined and filtered. As a result, 25 papers published between 2012 and 2022 were included in the analysis because they satisfied the requirements. The IoT sector has been fighting back for many years by allowing IoT security tools that shield systems and devices from threats and breaches, according to findings. Over the past few years, researchers from more interdisciplinary fields and geographically dispersed nations have begun to pay much more attention to IoT network security.

IoT frequently offers the data gathering, administration, and device and data protection services needed for application development. IoT things or gadgets interact and compute to improve the security and comfort of lives. IoT can be used for inventory automation, real-time item monitoring, and the administration of the information and state of things. The vast quantity of data that moves between the devices in the network necessitates the creation of a security structure that guarantees the integrity, secrecy, authentication, and permission of data. Studies have focused on using various methods to improve verification by various systems, including wireless ones.

There is still much room for improvement in the field of IoT security. Researchers need to be concerned in the area because of numerous ongoing studies and difficulties. High-security edge devices, the need for adequate shielding procedures and end-to-end encryption algorithms, secure fog-cloud computation, and improving the fog layers through machine learning and optimization methods such as deep learning and AI are some of the open challenges in IoT security. Blockchain is severely limited when there are many servers. Some highly efficient methods can replace nodes, and using numerous resources can emerge as a popular way to address the problem. Therefore, upcoming works can focus on various technologies like machine learning, AI, blockchain, etc.

Funding: This research received no external funding.

Data Availability Statement: Data sharing not applicable.

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

References

1. Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. *Sensors* **2019**, *19*, 2007. [CrossRef] [PubMed]
2. Patel, K.K.; Patel, S.M.; Scholar, P. Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. *Int. J. Eng. Sci. Comput.* **2016**, *6*, 6122–6131.
3. Hammoudi, S.; Aliouat, Z.; Harous, S. Challenges and research directions for Internet of Things. *Telecommun. Syst.* **2018**, *67*, 367–385. [CrossRef]
4. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
5. Taherdoost, H. Blockchain-Based Internet of Medical Things. *Appl. Sci.* **2023**, *13*, 1287. [CrossRef]
6. Chaudhary, S.; Johari, R.; Bhatia, R.; Gupta, K.; Bhatnagar, A. CRAIoT: Concept, review and application (s) of IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–4.
7. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access* **2021**, *9*, 28177–28193. [CrossRef]
8. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* **2020**, *20*, 3625. [CrossRef]
9. Hamad, S.A.; Sheng, Q.Z.; Zhang, W.E.; Nepal, S. Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1372–1391. [CrossRef]
10. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A. A Review of Security in Internet of Things. *Wirel. Pers. Commun.* **2019**, *108*, 325–344. [CrossRef]
11. Adat, V.; Gupta, B.B. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommun. Syst.* **2018**, *67*, 423–441. [CrossRef]
12. Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
13. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
14. Narayanan, U.; Paul, V.; Joseph, S. Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. *J. Ambient Intell. Humaniz. Comput.* **2021**, *13*, 769–787. [CrossRef]
15. Ahmed, M.I.; Kannan, G. Cloud-Based Remote RFID Authentication for Security of Smart Internet of Things Applications. *J. Inf. Knowl. Manag.* **2021**, *20*, 2140004. [CrossRef]
16. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. *Comput. Commun.* **2021**, *166*, 154–164. [CrossRef]
17. Anuradha, M.; Jayasankar, T.; Prakash, N.; Sikkandar, M.Y.; Hemalakshmi, G.; Bharatiraja, C.; Britto, A.S.F. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocess. Microsyst.* **2021**, *80*, 103301. [CrossRef]

18. Irshad, A.; Usman, M.; Chaudhry, S.A.; Bashir, A.K.; Jolfaei, A.; Srivastava, G. Fuzzy-in-the-Loop-Driven Low-Cost and Secure Biometric User Access to Server. *IEEE Trans. Reliab.* **2020**, *70*, 1014–1025. [CrossRef]
19. Chaudhry, S.A.; Farash, M.S.; Kumar, N.; Alsharif, M.H. PFLUA-DIoT: A pairing free lightweight and unlinkable user access control scheme for distributed IoT environments. *IEEE Syst. J.* **2020**, *16*, 309–316. [CrossRef]
20. Mishra, N.; Pandya, S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. *IEEE Access* **2021**, *9*, 59353–59377. [CrossRef]
21. Hameed, A.; Alomary, A. Security issues in IoT: A survey. In Proceedings of the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 22–23 September 2019; pp. 1–5.
22. Lu, Y.; Da Xu, L. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet Things J.* **2019**, *6*, 2103–2115. [CrossRef]
23. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
24. Jurcut, A.; Niculcea, T.; Ranaweera, P.; Le-Khac, N.-A. Security Considerations for Internet of Things: A Survey. *SN Comput. Sci.* **2020**, *1*, 1–19. [CrossRef]
25. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
26. Sha, K.; Yang, T.A.; Wei, W.; Davari, S. A survey of edge computing-based designs for IoT security. *Digit. Commun. Netw.* **2020**, *6*, 195–202. [CrossRef]
27. Yousefnezhad, N.; Malhi, A.; Främling, K. Security in product lifecycle of IoT devices: A survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102779. [CrossRef]
28. Yugha, R.; Chithra, S. A survey on technologies and security protocols: Reference for future generation IoT. *J. Netw. Comput. Appl.* **2020**, *169*, 102763. [CrossRef]
29. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ.-Comput. Inf. Sci.* **2018**, *30*, 291–319.
30. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27. [CrossRef]
31. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [CrossRef]
32. 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]
33. Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. Integration of Cloud computing and Internet of Things: A survey. *Futur. Gener. Comput. Syst.* **2016**, *56*, 684–700. [CrossRef]
34. HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A survey on internet of things security: Requirements, challenges, and solutions. *Internet Things* **2021**, *14*, 100129. [CrossRef]
35. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984. [CrossRef]
36. Romkey, J. Toast of the IoT: The 1990 Interop Internet Toaster. *IEEE Consum. Electron. Mag.* **2016**, *6*, 116–119. [CrossRef]
37. Rajaraman, V. Radio frequency identification. *Resonance* **2017**, *22*, 549–575. [CrossRef]
38. Yang, G. An Overview of Current Solutions for Privacy in the Internet of Things. *Front. Artif. Intell.* **2022**, *5*, 812732. [CrossRef]
39. Yu, T.; Sekar, V.; Seshan, S.; Agarwal, Y.; Xu, C. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks, Philadelphia, PA, USA, 16–17 November 2015; pp. 1–7.
40. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.
41. Nieles, M.; Dempsey, K.; Pillitteri, V.Y. An introduction to information security. *NIST Spec. Publ.* **2017**, *800*, 101. [CrossRef]
42. Russell, B.; Van Duren, D. *Practical Internet of Things Security*; Packt Publishing Ltd: Birmingham, UK, 2016.
43. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1636–1675. [CrossRef]
44. Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics* **2022**, *11*, 2181. [CrossRef]
45. Aldweesh, A.; Derhab, A.; Emam, A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowl.-Based Syst.* **2020**, *189*, 105124. [CrossRef]
46. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]
47. Pereira, T.; Barreto, L.; Amaral, A. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manuf.* **2017**, *13*, 1253–1260. [CrossRef]
48. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.

49. Moyne, J.; Mashiro, S.; Gross, D. Determining a security roadmap for the microelectronics industry. In Proceedings of the 2018 29th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC), Saratoga Springs, NY, USA, 30 April–3 May 2018; pp. 291–294.
50. Benias, N.; Markopoulos, A.P. A review on the readiness level and cyber-security challenges in Industry 4.0. In Proceedings of the 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Kastoria, Greece, 23–25 September 2017; pp. 76–80, ISBN 978-618-83314-0-2.
51. Hassanzadeh, A.; Modi, S.; Mulchandani, S. Towards effective security control assignment in the Industrial Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 795–800. [CrossRef]
52. Autenrieth, P.; Lörcher, C.; Pfeiffer, C.; Winkens, T.; Martin, L. Current significance of IT-infrastructure enabling industry 4.0 in large companies. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018; pp. 1–8.
53. Esposito, C.; Castiglione, A.; Martini, B.; Choo, K.-K.R. Cloud Manufacturing: Security, Privacy, and Forensic Concerns. *IEEE Cloud Comput.* **2016**, *3*, 16–22. [CrossRef]
54. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Kitchenham: Durham, UK, 2007.
55. Taherdoost, H. Non-Fungible Tokens (NFT): A Systematic Review. *Information* **2023**, *14*, 26. [CrossRef]
56. Abu Saa, A.; Al-Emran, M.; Shaalan, K. Factors Affecting Students' Performance in Higher Education: A Systematic Review of Predictive Data Mining Techniques. *Technol. Knowl. Learn.* **2019**, *24*, 567–598. [CrossRef]
57. de Lacalle, L.N.L.; Posada, J. Special issue on new Industry 4.0 advances in industrial IoT and visual computing for manufacturing processes. *Appl. Sci.* **2019**, *9*, 4323. [CrossRef]
58. Tayyaba, S.; Khan, S.A.; Tariq, M.; Ashraf, M.W. Network security and Internet of things. In *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*; IGI Global: Hershey, PA, USA, 2020; pp. 198–238.
59. Logrippo, L. Multi-level models for data security in networks and in the Internet of things. *J. Inf. Secur. Appl.* **2021**, *58*, 102778. [CrossRef]
60. El-Latif, A.A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E.; Elwahsh, H.; Piran, J.; Bashir, A.K.; Song, O.-Y.; Mazurczyk, W. Providing End-to-End Security Using Quantum Walks in IoT Networks. *IEEE Access* **2020**, *8*, 92687–92696. [CrossRef]
61. Li, Y.; Sha, J.; Geng, R. Research on internal network data security monitoring method based on NB-IOT. *Web Intell.* **2021**, *19*, 191–202. [CrossRef]
62. Batra, I.; Verma, S.; Kavita; Alazab, M. A lightweight IoT-based security framework for inventory automation using wireless sensor network. *Int. J. Commun. Syst.* **2020**, *33*, e4228. [CrossRef]
63. Kalyani, G.; Chaudhari, S. Cross Layer Security MAC Aware Routing Protocol for IoT Networks. *Wirel. Pers. Commun.* **2022**, *123*, 935–957. [CrossRef]
64. Ali, F.; Mathew, S. An efficient multilevel security architecture for blockchain-based IoT networks using principles of cellular automata. *PeerJ Comput. Sci.* **2022**, *8*, e989. [CrossRef] [PubMed]
65. Kaňuch, P.; Macko, D. E-HIP: An Energy-Efficient OpenHIP-Based Security in Internet of Things Networks. *Sensors* **2019**, *19*, 4921. [CrossRef] [PubMed]
66. Parne, B.L.; Gupta, S.; Chaudhari, N.S. SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network. *IEEE Access* **2018**, *6*, 3668–3684. [CrossRef]
67. Tao, M.; Ota, K.; Dong, M.; Qian, Z. AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks. *J. Parallel Distrib. Comput.* **2018**, *118*, 107–117. [CrossRef]
68. Pan, M.; Tian, S.; Yuan, J.; Chen, S. Simulation of Dynamic User Network Connection Anti-Interference and Security Authentication Method Based on Ubiquitous Internet of Things. *Math. Probl. Eng.* **2021**, *2021*, 1–8. [CrossRef]
69. Medhane, D.V.; Sangaiah, A.K.; Hossain, M.S.; Muhammad, G.; Wang, J. Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach. *IEEE Internet Things J.* **2020**, *7*, 6143–6149. [CrossRef]
70. Zhang, Q.; Xu, D. Security authentication technology based on dynamic Bayesian network in Internet of Things. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 573–580. [CrossRef]
71. Sankar, S.P.; Subash, T.D.; Vishwanath, N.; Geroge, D.E. Security improvement in block chain technique enabled peer to peer network for beyond 5G and internet of things. *Peer Netw. Appl.* **2021**, *14*, 392–402. [CrossRef]
72. Hu, B.; Tang, W.; Xie, Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments. *Neurocomputing* **2022**, *500*, 741–749. [CrossRef]
73. Shahid, H.; Ashraf, H.; Javed, H.; Humayun, M.; Jhanjhi, N.; AlZain, M.A. Energy Optimised Security against Wormhole Attack in IoT-Based Wireless Sensor Networks. *Comput. Mater. Contin.* **2021**, *68*, 1967–1981. [CrossRef]
74. Verma, S.; Kawamoto, Y.; Kato, N. A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices. *IEEE Internet Things J.* **2021**, *8*, 8411–8422. [CrossRef]
75. Wu, F.; Xu, L.; Kumari, S.; Li, X. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security. *J. Ambient. Intell. Humaniz. Comput.* **2017**, *8*, 101–116. [CrossRef]

76. Yu, H.; He, J.; Liu, R.; Ji, D. On the Security of Data Collection and Transmission from Wireless Sensor Networks in the Context of Internet of Things. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 806505. [CrossRef]
77. Xie, S.; Wang, X.; Shang, H. Security Analysis on Wireless Sensor Network in the Data Center for Energy Internet of Things. *Int. J. Saf. Secur. Eng.* **2020**, *10*, 397–402. [CrossRef]
78. Sun, N.; Li, T.; Song, G.F.; Xia, H.R. Network Security Technology of Intelligent Information Terminal Based on Mobile Internet of Things. *Mob. Inf. Syst.* **2021**, *2021*, 6676946. [CrossRef]
79. Deng, Z.; Li, Q.; Zhang, Q.; Yang, L.; Qin, J. Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network With SWIPT. *IEEE Internet Things J.* **2019**, *6*, 10786–10798. [CrossRef]
80. Teng, D. Industrial Internet of Things Anti-Intrusion Detection System by Neural Network in the Context of Internet of Things for Privacy Law Security Protection. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–17. [CrossRef]
81. Yin, X.C.; Liu, Z.G.; Ndibanje, B.; Nkenyereye, L.; Islam, S.M.R. An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks. *Sensors* **2019**, *19*, 3146. [CrossRef]
82. Manimuthu, A.; Ramesh, R. Privacy and data security for grid-connected home area network using Internet of Things. *IET Netw.* **2018**, *7*, 445–452. [CrossRef]
83. Boussard, M.; Bui, D.T.; Douville, R.; Justen, P.; Le Sauze, N.; Peloso, P.; Vandeputte, F.; Verdot, V. Future Spaces: Reinventing the Home Network for Better Security and Automation in the IoT Era. *Sensors* **2018**, *18*, 2986. [CrossRef] [PubMed]
84. Khan, N.A.; Awang, A.; Karim, S.A.B.A. Security in Internet of Things: A Review. *IEEE Access* **2022**, *10*, 104649–104670. [CrossRef]
85. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. [CrossRef] [PubMed]

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.