sustainability

MDPI

Review

Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective

Firuz Kamalov [1], Behrouz Pourghebleh [2], Mehdi Gheisari [1,3,4,5,*], Yang Liu [3] and Sherif Moussa [1]

[1] Department of Electrical Engineering, Canadian University Dubai, Dubai 144534, United Arab Emirates
[2] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz 5157944533, Iran
[3] Department of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China
[4] Department of Cognitive Computing, Institute of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India
[5] Young Researcher and Elite Club, Parand Branch, Islamic Azad University, Parand 182125, Iran
* Correspondence: mehdi.gheisari61@gmail.com

Abstract: The Internet of Medical Things (IoMT), an application of the Internet of Things (IoT) in the medical domain, allows data to be transmitted across communication networks. In particular, IoMT can help improve the quality of life of citizens and older people by monitoring and managing the body's vital signs, including blood pressure, temperature, heart rate, and others. Since IoMT has become the main platform for information exchange and making high-level decisions, it is necessary to guarantee its reliability and security. The growth of IoMT in recent decades has attracted the interest of many experts. This study provides an in-depth analysis of IoT and IoMT by focusing on security concerns from different points of view, making this comprehensive survey unique compared to other existing studies. A total of 187 articles from 2010 to 2022 are collected and categorized according to the type of applications, year of publications, variety of applications, and other novel perspectives. We compare the current studies based on the above criteria and provide a comprehensive analysis to pave the way for researchers working in this area. In addition, we highlight the trends and future work. We have found that blockchain, as a key technology, has solved many problems of security, authentication, and maintenance of IoT systems due to the decentralized nature of the blockchain. In the current study, this technology is examined from the application fields' points of view, especially in the health sector, due to its additional importance compared to other fields.

Keywords: Internet of Medical Things; privacy; security; information technology; Internet of Things

Citation: Kamalov, F.; Pourghebleh, B.; Gheisari, M.; Liu, Y.; Moussa, S. Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective. *Sustainability* **2023**, *15*, 3317. https://doi.org/10.3390/su15043317

Academic Editor: Zubair Baig

Received: 14 November 2022
Revised: 5 February 2023
Accepted: 7 February 2023
Published: 10 February 2023

1. Introduction

The Internet is a vast information network and database that is now intertwined with various aspects of life. With the advancement of science and technology, the Internet and computer network technologies have affected the economy, military, and politics [1]. With the advent of the Internet, human communication has undergone a fundamental revolution. Therefore, these communications have entered a new phase of communication. In the emerging stage of the Internet, communication is no longer limited to humans. Instead, it is about intelligent, interconnected devices that gave rise to the Internet of Things (IoT) concept. More than a decade has passed since the introduction of the concept of IoT. It aims to link various devices over the Internet. An IoT device is a system that incorporates sensors, actuators, or both. It connects to the Internet directly or through another component [2]. It opens up possibilities for directly integrating the physical world with computer-based systems. Systems, such as smart cars, refrigerators, and homes are mentioned in various topics these days. The International Telecommunication Union defines IoT as an infrastructure that combines physical and virtual devices. The IoT finds its application in almost any field to provide an advanced mode of communication between different devices and systems

and to facilitate human interaction with the virtual environment. It is now a prevalent topic of discussion between researchers and professionals. It is considered a universal presence since it allows all objects/things in our environment to be linked via the Internet and to communicate without human need. The adoption of IoT applications is spreading worldwide; western Europe, North America, and China are the key driving countries [1]. Machine-to-machine (M2M) connections will increase from 5.6 billion in 2016 to 27 billion in 2024. The IoT market is predicted to expand from $892 billion in 2018 to $4 trillion by 2025 [3]. Many corporations and technological giants (including Intel, Microsoft, Cisco, and Inter Digital) have realized the economic value of IoT and are working hard to make it a reality. The number of IoT devices has exponentially exploded in recent decades [4]. Several applications of it in different sectors are as follows (Table 1).

Table 1. Several applications of IoT in different sectors.

Business	Industry	Medical and Treatment
Theft protection	Real-time information about the performance of the machines used	Increasing the quality of patient care
Send and launch personal offers	Monitor material availability	Improves resource allocation decisions Improves physician–patient relationship
Support in marketing activities, communication, and transactions	Controls energy consumption	Smart hospitals, smart homes, intelligent automobiles, intelligent dispersed networks, smart manufacturing industries, smart grids, and virtual learning environments are examples of IoT landscapes and devices spread across our society.
More appropriate product control	Improves production processes	

Following the review and comparison of the current study with previous studies by reviewing the literature, the novel contributions of this study in summary are as follows:

(1) Classification of studies conducted in improving security in IoT and IoMT according to different application fields.
(2) After classifying studies according to different application fields, we compare and evaluate the collected studies from different aspects, including the fields of application, year of publication, publisher, and so on, in schematic form.
(3) The classification of studies based on the most important approach used in improving security according to their main application contexts.
(4) Identifying approaches to maintain and improve security in IoT.
(5) Blockchain technology is also investigated in this study, especially in the medical field.

Research Questions

The authors' perspective of the current research study is to provide a comprehensive overview of security in the IoT and IoMT and examine the practical aspects that can serve as a search engine for easy access to scientific and research documentation. In this regard, the review analysis conducted in this field is based on the following research questions:

(1) What is the classification and comparison of the most important areas of security work in IoT?
(2) What is the most important approach used to enhance security in IoMT?
(3) What are the application areas of the blockchain approach and its classification?
(4) What are the application areas of the blockchain approach in the health field?

In the next step, we identify the most important and latest approaches to improve security in IoMT.

The rest of the paper is organized in the following manner. Section 2 describes IoT, its definition, characteristics, and architecture. Section 3 describes the Internet of Medical Things. Section 4 contains the blockchain and its application. Finally, Section 5 concludes this research and explains future trends.

2. IoT Architecture and Applications

Figure 1 depicts a four-layer service-oriented architecture of IoT in terms of its functions [5,6].

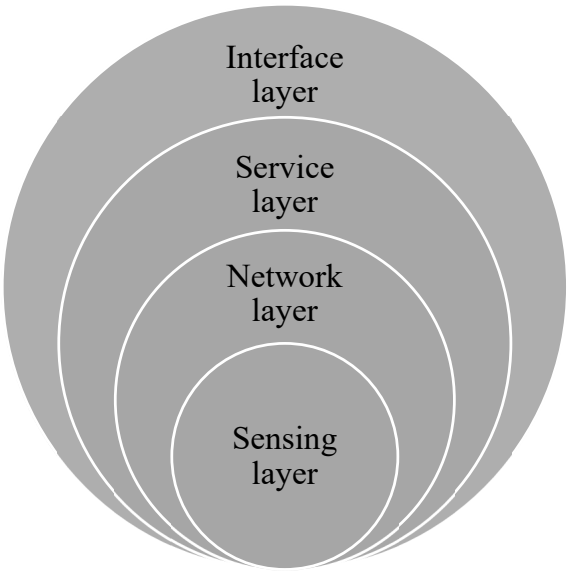

Figure 1. Four-layered service-oriented architecture of IoT [2].

As shown in Figure 1, to have a fully service-oriented IoT architecture, four layers should be included, namely the sensing layer, network layer, service layer, and interface layer.

2.1. Research Process

The research process of this study consisted of six search stages. The search was performed on well-known online databases, such as IEEE, ScienceDirect, Springer, MDPI, Google Scholar, etc. The search approach used in the current study is shown in Figure 2, which has the following steps.

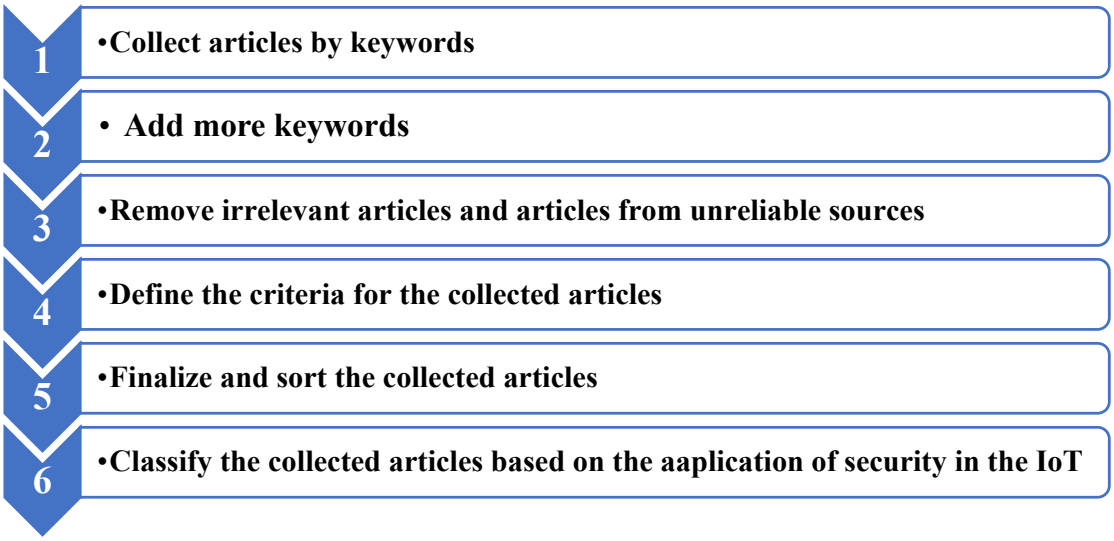

Figure 2. Research process.

Step 1: Collect articles by keywords

In order to provide more accurate results and compare the results, in this section, we consider IoMT and IoT applications in other domains. This step was performed in the first stage of collecting articles by using the following keywords:

("IoT" and "Transportation"),	("IoT" and "Medical")
("IoT" and "Business")	("IoT" and "Military")
("IoT" and "Education")	("IoT" and "Manufacturing" or "Industry")
("IoT" and "Smart Cities")	("IoT" and "Smart Grids")
("IoT" and "Agriculture")	("IoT" and "Smart Home")
("IoT" and "Supply Chain")	("IoT" and "Banking System")

A total of 1233 articles were collected using these keywords and by searching databases.

Step 2: Add more keywords

The first task is classifying security-related articles in the IoT by their field of application, including IoMT, E-healthcare, and others. In the second step of the search process, we filter the articles collected in the previous step by adding more keywords. We used the following keywords:

("IoT" and "Security" and "Transportation")	("IoT" and "Security" and "Medical")
("IoT" and "Security" and "Business")	("IoT" and "Security" and "Military")
("IoT" and "Security" and "Education")	("IoT" and "Security" and "Manufacturing" or "Industry")
("IoT" and "Security" and "Smart Cities")	("IoT" and "Security" and "Smart Grids")
("IoT" and "Security" and "Agriculture")	("IoT" and "Security" and "SmartHome"),
("IoT" and "Security" and "Supply Chain")	("IoT" and "Security" and "Banking Systems")

Upon filtering and modifying the search, the number of articles collected in the previous step was reduced to 641.

Step 3: Remove irrelevant articles and articles published on unreliable sites

At this stage of the search process, through reading the abstract, articles irrelevant to the current study, articles from unreliable sources, and duplicate articles were removed. As a result, 275 of 641 articles filtered in the previous stage were obtained as articles in line with the research topic and published in valid databases.

Step 4: Define the criteria for the collected articles:

At this stage, to further improve the results that have been filtered so far, we considered additional criteria for retaining articles as follows:

Criterion 1—Articles that include security applications in IoT (generalized point of view), especially in the medical field.
Criterion 2—Articles published in invalid databases.

Finally, after filtering according to the above criteria, we obtained 147 articles.

Step 5: Finalize and sort the collected articles

We used databases, keywords, and retention criteria to remove irrelevant and duplicate articles. We then ensured that the remaining articles were relevant to applying IoT (generalized point of view). On the other hand, at this point during this search process, we were sure that the collected articles were not impartial and biased, and we entered the next stage, which was one of the most important parts of the current study.

2.1.1. Research on IoT from Different Perspectives

In this section, we investigate IoT from different points of view, including years and well-known publishers. This analysis and comparison benefits researchers in academia and industry, especially new researchers.

2.1.2. Analysis Based on the Year of Publication of Articles

Considering the above, we have decided to categorize the collected articles in network security based on the years of publication in this section. This classification shows a growing trend in interest regarding IoT security. The number of articles published on IoT security has been growing from 2011 to 2022 (Figure 3).

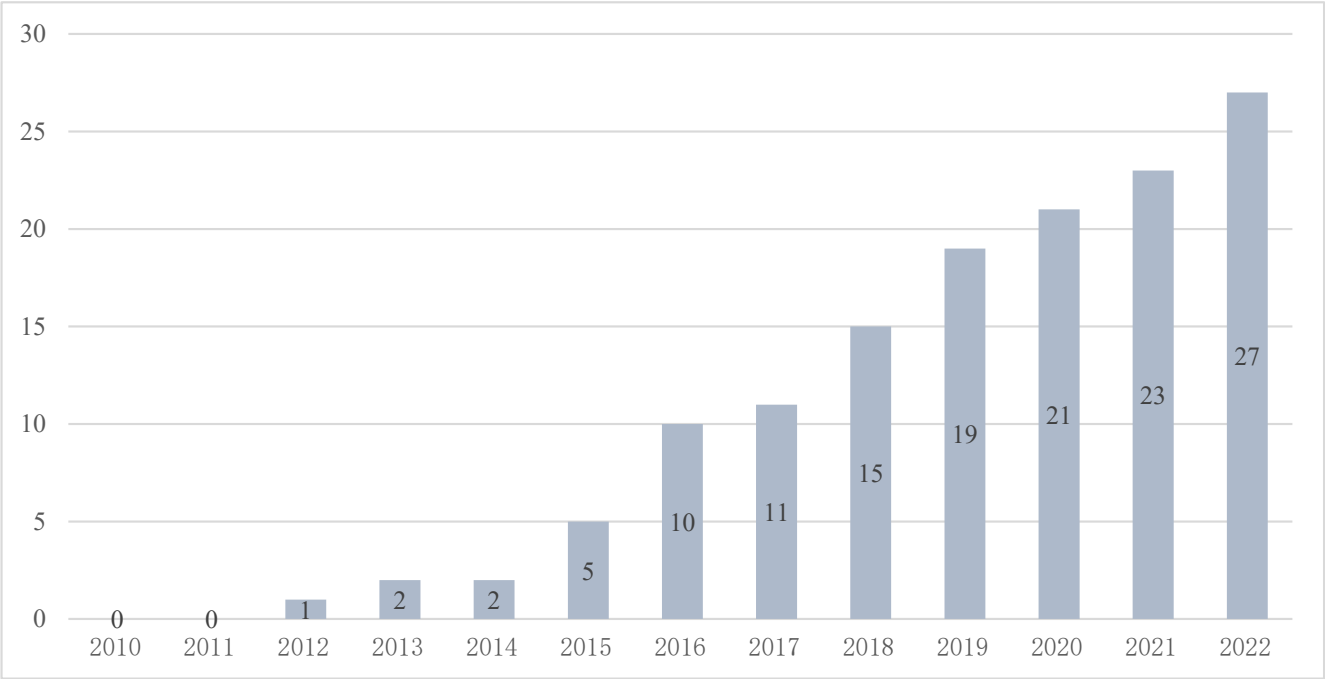

Figure 3. Article publication years.

In other words, the need for security has doubled with the increasing use of IoT in various fields and its impact on different aspects of life. Therefore, this issue has become a significant challenge that has attracted the attention of many researchers. Every year, many researchers aim to provide solutions to maintain and improve security in IoT.

2.1.3. IoT Publication Analysis

According to a wide range of scientific journals around the world and following the reviews of IoT-related research papers, in this section, we review the journals that publish research papers in this field and related topics. Some leading journals in this field can be seen in Figure 4.

Considering Figure 4, it is clear that the IEEE has been at the forefront of publishing security in IoT research over other journals. Springer is the second-largest publisher of IoT security articles. Concerning Figure 4, the chart highlights the journals that have led the way in publishing IoT security publications over other journals. According to the sample, 136 articles gathered for this study are shown between 2010 and 2022. Comparison based on the publishers shows how active they are, which leads to this result. For example, Emerald does not seem interested in publishing papers about IoT too much. Thus, authors can ignore it and submit their works elsewhere.

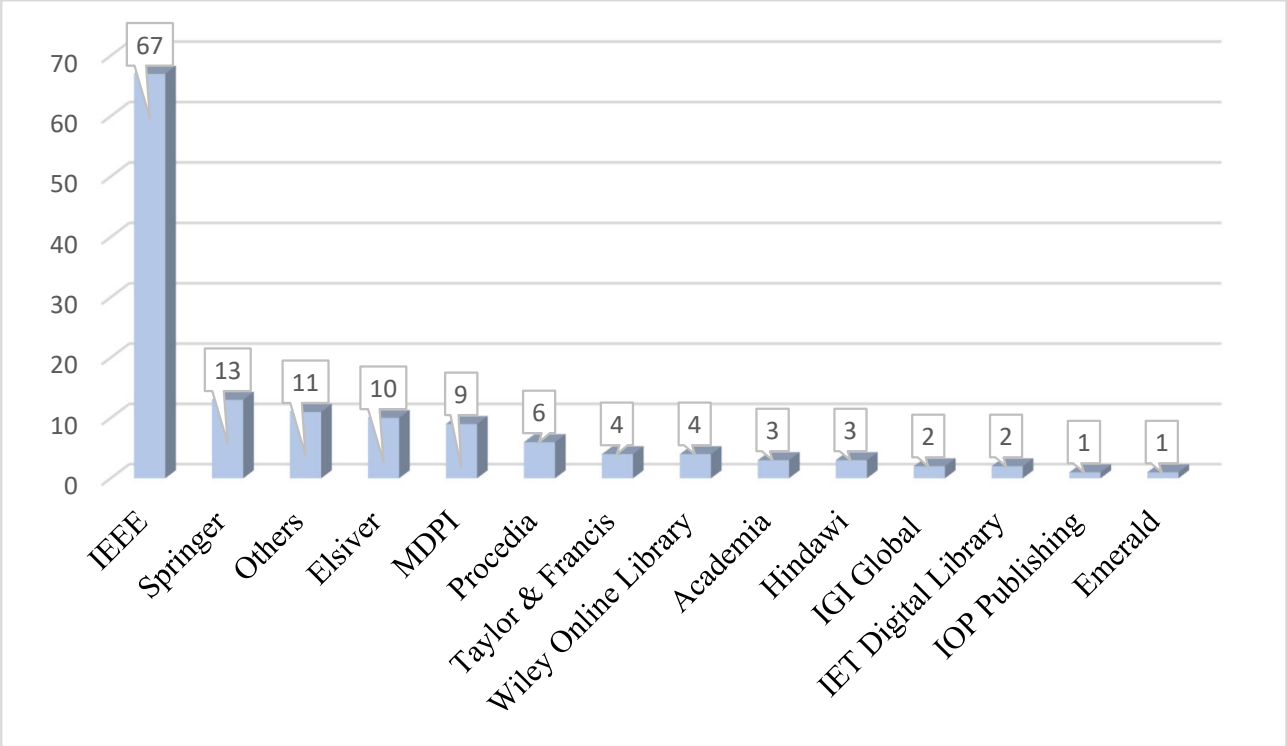

Figure 4. IoT publishers.

2.2. Analysis of IoT Security in Different Domains

When we are in intelligent environments and technologies, such as IoT, we must spend extra time and energy recognizing security challenges and solutions. In other words, since all objects use the Internet infrastructure to exchange information, it has exposed various security issues. Multiple reasons have led to the slow development of this concept, such as the lack of development of required technologies and security challenges.

Security has been introduced as one of the fundamental challenges of IoT. This issue happens because of the unique nature of security and its implementation in IoT networks, which differ from regular wired and wireless networks. The main reasons for the need for IoT security are as follows [7–9]:

(1) The IoT is a multifunctional paradigm with many applications and requirements. This nature illustrates the enormous complexity of such systems through broad IoT implementations.
(2) IoT systems are immensely varied in protocols, platforms, and devices available globally, mainly comprising restricted resources, lossy connectivity, and lack of standardization.
(3) IoT devices are mostly configured to self-adapt to their environment. An effective IoT security solution that secures each device separately and provides an end-to-end security solution must be presented.

In the first phase, research studies on IoT security were gathered. As a result, from 2010 to 2022, about 136 papers on this topic were collected. The published publications in high-quality journals were divided into 12 categories based on the application area.

2.2.1. Articles Collected for Each Application

In this section, we examine other IoT application fields. Thus, the collected articles were independently divided into groups based on their application. The categorization can be seen in Table 2. In order to make a transparent review and comparison, these reviews and comparisons are made in the form of figures.

Table 2. Category of collected articles.

No	Applications	References
1	IoT security and medical	[10–49]
2	IoT security and transportation	[50–65]
3	IoT security and business	[66–71]
4	IoT security and military	[72–81]
5	IoT security and education	[82–87]
6	IoT security and industry	[88–90]
7	IoT security and smart cities	[91–103]
8	IoT security and smart grid	[104–113]
9	IoT security and agriculture	[114–124]
10	IoT security and smart home	[125–134]
11	IoT security and supply chain	[135–142]
12	IoT security and banking system	[143,144]

Figure 5 shows the number of articles collected for each listed application. The trend shown in this diagram shows the importance and scope of IoT security applications. It is clear from the figure that security for IoT in medical contexts has been more focused than in other areas.

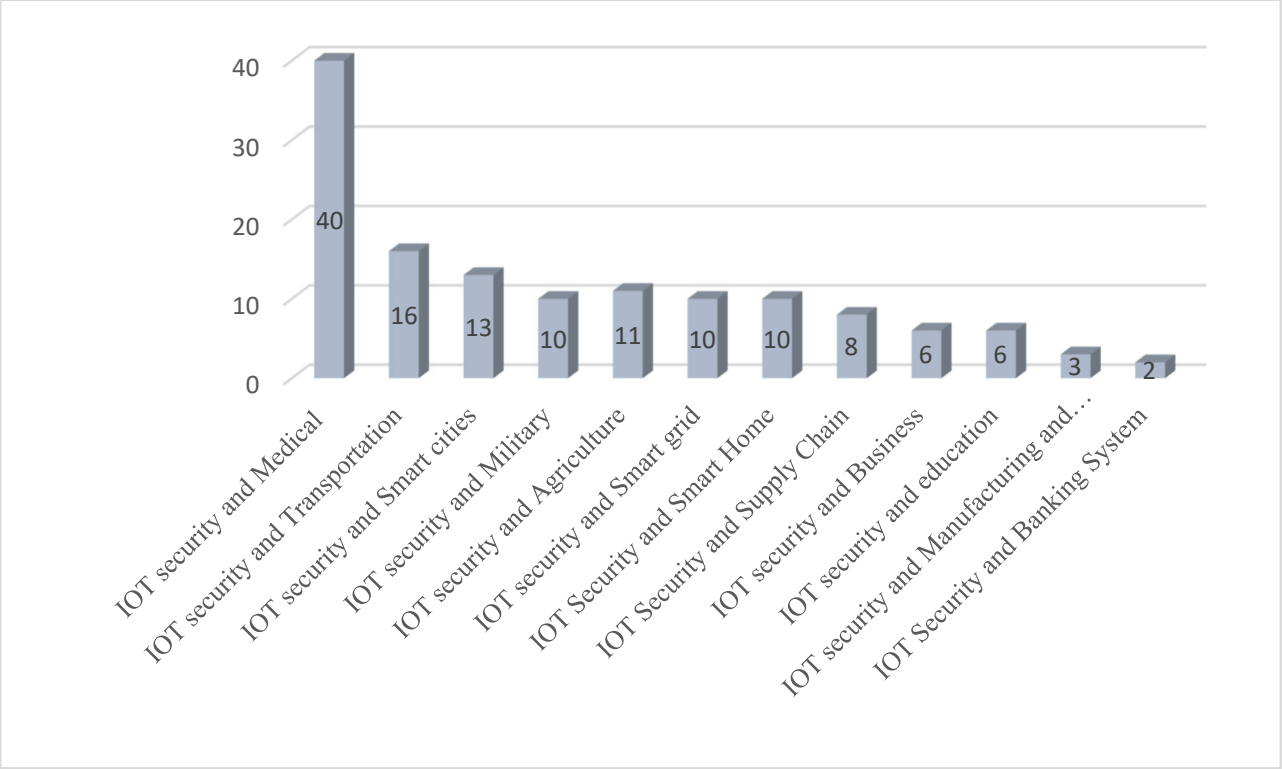

Figure 5. Articles in various applications.

2.2.2. Leveraged Approaches in IoT Security Applications

In this section, we review the approaches used in IoT security. This review can be seen in the form of Table 3. It shows the approaches that each IoT application is using. In this table, the number of articles in each category is specified.

Table 3. Review of the approaches used in IoT security.

Approach \ Category	IoT Security and Transportation	IoT Security and Medical	IoT Security and Business	IoT Security and Military	IoT Security and Education	IoT Security and Industry	IoT Security and Smart Cities	IoT Security and Smart Grid	IoT Security and Agriculture	IoT Security and Smart Home	IoT Security and Supply Chain	IoT Security and Banking System
Artificial Intelligence	3	5					4			1		1
Fuzzy	1										1	
Field programmable gate array	1											
Blockchain technology	2	1				1	1		2	1	1	1
Geospatial modelling approach	1											
Intrusion detection System	1											
Game theory approach	1											
Prioritization rules	1											
Global Positioning System (GPS)	2											
Cyber-physical systems	1											
Cloud technologies	2					1		1				
Authentication and anonymity		6										
Symmetric cryptography		1										
Embedded encryption algorithm		3										
Architecture analysis		1										
End-to-end security scheme		1										
The security scheme of 6LoWPAN		2						1				
Vulnerable software processes		2										
System-theoretic process analysis		1										
Deep learning (DL) algorithms		2					1					
Risk assessment		3										
Lightweight Protocol		2										
Context-sensitive to access control		1										
Fog computing		2										
Markov model			1									
Information security modelling			1									
Conceptual modeling			1				1					
Encryption method			1			1						
Cryptographic access control				3							1	
Security evaluation with risk management				1								
Security evaluation on multi-metric approach				1								
The systemic and cognitive approach				1								

Table 3. *Cont.*

Approach \ Category	IoT Security and Transportation	IoT Security and Medical	IoT Security and Business	IoT Security and Military	IoT Security and Education	IoT Security and Industry	IoT Security and Smart Cities	IoT Security and Smart Grid	IoT Security and Agriculture	IoT Security and Smart Home	IoT Security and Supply Chain	IoT Security and Banking System
Wireless sensor network with authentication				1								
Fault tolerance mechanisms				1				1				
Encryption algorithm					1							
ANTcentric security					1		1					
Policy-based secure and trustworthy sensing							1					
SMARTIE project approach							1					
AAA-protected network							1					
Trusted secure access control system								1				
5G cellular networks								1				
Monte Carlo simulations								1				
Edge computing								1				
Raspberry Pi board and an array of sensors									1			
New algorithm to control Security									1			
System block diagram									1			
IR sensor and GSM module									1			
AllJoyn framework										1		
Software-defined networking										1		
Z-Wave										1		
Mapping the security											1	
Lightweight improved protocol on authenticated encryption											1	
IoT-based secured decision making management approach											1	
Risk management model											1	
Other methods		5	2	2	4		2	3	1	1		

As mentioned earlier, the primary goal of this research is to examine previous studies on IoMT security and its nearby applications. In this regard, after collecting scientific articles, we entered the stage of interpretation and study. To perform this step and create comfortable and transparent evaluations, we decided to perform the interpretations in graphs at this stage. The IoT security papers are leveraging several well-known approaches, including artificial intelligence (AI), blockchain technology, fog computing, intrusion detection systems, cyber-physical systems, cloud technologies, authentication and anonymity, encryption method, encrypting communications, edge computing, the 6LoWPAN technique, and 5G cellular networks. In order to explain this diagram, it can be stated that each of the collected articles was studied in 12 categories in Table 2 to identify the adopted approach. These articles were re-categorized in each category based on IoT Security upgrade approaches. For this purpose, in Table 3, 40 articles are considered based on the approach used in the column related to medical applications. It is clear from this column that six articles have used the "Authentication and Anonymity" approach, five articles use the "AI" approach, three articles use the "embedded encryption algorithm" approach, and so on. The above review was performed for each of the 12 categories formed for the "IoT and IoMT Security method". After identifying these approaches in all articles as shown in Table 3, in many cases, the "privacy analysis" and "IoT security" using the "AI" approach have grabbed the interest of many researchers. The following is a brief introduction to this topic.

In this context, AI is a new technology science that simulates and extends human thought processes, methods, technology, and applications. Furthermore, AI can be divided into three categories, namely weak AI, strong AI, and super AI. Machine learning (ML), natural language processing (NLP), robots, computer vision, and expert systems are some of the key technologies of AI. Of these, ML is one of the most important AI technologies. It analyzes a large quantity of data to identify potential laws that can be used to guide human decision making. Deep learning (DL) is considered to be the most representative branch of machine learning. It has a multilayer perceptron structure containing multiple hidden layers, which facilitates the discovery of deeper rules in the data and provides robust feature extraction. The most common deep learning models are the convolutional neural network (CNN), the deep belief network (DBN), and the stacked autoencoder network (SAN). This ML technology can be used in the medical field to identify and diagnose diseases, which largely avoids the high error rate, low efficiency, and the emergence of many diseases associated with inaccurate diagnosis.

In medical treatment, AI technology is bringing technological innovation and altering the way that medical services are provided.

3. Internet of Medical Things

Many regions of the world face a great challenge in managing rapidly aging populations, people with chronic diseases, child mortality, frequent outbreaks of disease epidemics, harsh living environments with poor mental health, lack of drinking water resources, and increasing pollution. Although the global demand for medical services has increased in recent years, we still live in the traditional hospital-based model of care, where citizens visit a physician when they are sick. To manage their chronic disease, patients frequently visit hospitals or clinics for doctors to perform observations that include monitoring disease progression as well as clinical decision making that leads to treatment adjustments. In general, hospitals use a disease- and physician-centered model that is more reactive and does not involve patients as an active part of the medical process. We briefly list some of the challenges and obstacles facing hospital-based medical practices, as follows:

(1) Limited time;
(2) Adherence monitoring;
(3) Aging population;
(4) Urbanization;
(5) Health care workforce shortage [145].

The IoT technology has affected medical systems in a way to support advanced medical services. The advancement of IoT technology has revolutionized how we enact activities that improve people's lives economically, professionally, and socially. The health sector cannot avoid using all these tools to benefit health care. Here, IoT-connected medical devices (Internet of Medical Things or IoMT) proactively report system drain information to operators to prevent device shutdowns. Remote monitoring can be effectively enabled with IoT-connected medical devices. Sensors attached to patients can record health data and then share this data with medical staff via wireless communication. As such, IoT technology in medical environments facilitates the management of the healthcare system and creates many possibilities for medical services, namely IoMT [146].

Here, IoMT is the connection of various medical devices and applications through computer networks. These devices allow direct communication between their servers and medical personnel. The data collected, stored, and processed by all these devices provide valuable information to humanity. Recent studies show that this information is the key to health care and prevents some diseases. Other scientific studies have shown that many diseases affecting humans are likely to be avoided by changing environments and lifestyles.

3.1. How IoMT Works

Data are collected and sent by the medical staff using computer devices and networks for analysis and storage in the cloud. After that, these data become information for personnel decision making.

There are a wide range of devices used in the health field, including the following:

- External portable devices; for example, devices that monitor blood pressure, glucose, temperature, etc.
- Implanted devices; for example, pacemakers, infusion pumps, drug delivery devices, glucose monitors, etc.
- Stationary medical devices; X-ray and magnetic resonance devices, patient monitoring [147].

3.2. Selected Current Studies on IoMT

In this section, to clarify current studies, we explain our reasons for selecting them, which are as follows:

The blockchain was examined by Alam and Shuaib [148] in conjunction with fog computing to mitigate the impact of health difficulties. According to this research, blockchain technology can potentially overcome the security concerns associated with fog computing.

Ullah and Khan [149] presented a multi-message and multi-receiver encryption strategy for an IoMT system. It ensures receivers' privacy, integrity, and anonymity in multicast channels under the random oracle model (ROM). To encrypt and authenticate signatures, the proposed scheme utilizes hyperelliptic curve cryptography.

Chaganti and Mourade [150] implemented a robust and reliable intrusion detection system in IoMT using a deep neural network and particle swarm optimization algorithm. The proposed system is more accurate than the existing methods, with a 97% accuracy rate in detecting network intrusions. Rahmani and Hosseini Mirmahaleh [151] developed a flexible clustering algorithm to classify the healthcare service providers in order to detect faults on time and select the appropriate servers to join the cluster by considering the priority of services and applications.

Alsubaei and Abuhussein [152] presented a taxonomy of IoMT security and privacy concerns based on various features of attackers, including difficulty, severity, source, method, impact, and compromise level. This taxonomy is updatable and expandable to cover new services, devices, and attacks. Hatzivasilis and Soultatos [153] presented a comprehensive analysis of basic security and privacy policies required in current IoMT scenarios to protect various stakeholders and users. The entire strategy can be regarded as a roadmap toward the safe deployment of IoMT systems, incorporating a circular economy. Sun, Lo [154] reviewed the security and privacy challenges and requirements of IoMT-based

healthcare systems from the data level to the medical server level. The use of biometrics in IoMT healthcare systems was also discussed. A discussion of security schemes for implantable IoMT devices is also discussed in this paper, as medical implantable devices suffer from unique hardware challenges.

Koutras and Stergiopoulos [155] classified IoT communication protocols, considering their applications in IoMT. Then, they described the key features of IoT communication protocols adopted at the different medical device layers. They examined the security characteristics and restrictions of IoMT-specific communication protocols. Based on realistic attacks, they identified existing mitigation controls that may be useful to secure IoMT communications and current research and implementation gaps. Ghubaish and Salman [156] presented novel methods for protecting IoMT data during gathering, exchange, and storage. Their comprehensive overview covers both physical and network attacks on IoMT systems. The study results revealed that most security techniques ignore various types of attacks. Therefore, they proposed a security model that integrates multiple security approaches. The model addresses most of the known attacks against IoMT security.

Comprehensively and systematically, Hameed and Hassan [157] discussed the IoMT security and privacy issues and how machine learning approaches can be used to address them. The designated research questions are addressed by analyzing the study's methodology, good features, limitations, tools, and datasets. The results of this study indicate that machine learning techniques can effectively address IoMT security issues. As attacks on devices, such as IMDs, threaten patients' health and well-being, most studies focus on device layer or body area network security. Security solutions include anomaly detection, authentication, and access control in such devices. Awotunde, Jimoh [158] presented an overview of IoT, outlining its architecture and revealing the IoT-based healthcare application security and privacy issues. Additionally, they proposed an approach to secure healthcare information in the IoT environment. The approach protects healthcare data on the IoT platform and meets the strict privacy and security requirements of ubiquitous medical requests.

Hasan and Ghazal [159] outlined vulnerabilities potentially compromising the security, reliability, and privacy of IoMT systems. Research has revealed that IoMT can be attacked in various ways, notably eavesdropping, malware, and DoS attacks. Furthermore, IoMT faces various threats, including confidentiality, privacy, and security. Cryptographic techniques are emerging to boost the reliability and security of IoMT devices, despite various security concerns. Sadhu and Yanambaka [160] present an overview of the IoMT ecosystem, its functions, and potential threats. In this study, the existing security solutions for resource-constrained IoT devices were analyzed in order to protect privacy and improve security. In addition, current authentication methods, such as ABE, ECC, MAC, ML, PUF, and blockchain were evaluated. Furthermore, NDN technology is also incorporated here, which is currently under investigation to enhance security. Papaioannou and Karageorgou [161] first categorized the existing and potential threats to IoMT edge network environments. These threats are classified according to key security objectives, such as availability, authorization, authentication, integrity, and confidentiality. A categorization of countermeasures against threats to IoMT edge networks was also provided. Generally, the study aims to provide researchers with insight into IoMT edge network threats and countermeasures. It also proposes a framework for organizing research efforts toward designing and developing lightweight security mechanisms that can overpower the limitations of IoMT devices in terms of resources and computation power while maintaining edge network security.

3.3. IoMT Privacy and Security Solutions

Over the last decade, several security and privacy solutions have been developed to prevent the negative use of IoMT. Indeed, IoT applications, such as IoMT, and devices are increasingly being attacked by cyber threats, highlighting the need to adopt some important practices to resolve these problems. These IoMT applications are more susceptible to security issues due to DOS attacks and other server attacks [162,163].

As IoMT technology is in the development phase and has not matured enough, it presents security risks due to a lack of user knowledge, poor maintenance, and inadequate standards. Hackers and adversaries can easily control IoMT devices with weak security by using malware for ransom [164,165]. Wearable devices, smart homes, and health-related applications are negatively affected by the control of IoMT devices. It is still necessary to carry out research in this area to make IoMT devices more secure from this type of attack. Companies launch products quickly and do not update the software promptly to remain competitive, making IoMT devices vulnerable to hacker attacks [166]. The link between a user's IoMT device and the cloud may break during an update. Hackers can access an unencrypted IoMT device through unencrypted communication. Upon a breakdown of the cloud connection, the organization will need to block ports and access immediately, and IoMT devices must be updated as necessary to remain secure [167]. Figure 6 explains the security areas of the IoMT schematically.

Figure 6. Security areas in IoMT.

As Figure 6 depicts, IoMT suffers from several security issues, such as applying security in patient monitoring or malware prevention.

4. Blockchain and Its Application

Blockchain (BC) systems are one of the most remarkable technologies in IoMT settings because they are a distributed sharing mechanism that allows IoMT devices to connect safely. A blockchain is a chain of blocks, and each block is linked to the blocks that come before it. Every block contains the security hash code, the preceding block hash, and the contents. Each block has a hash code that points to the previous block and another to the next block. Each block has a timestamp, a nonce, and a transaction history. The structure of the blockchain is shown in Figure 7 [168].

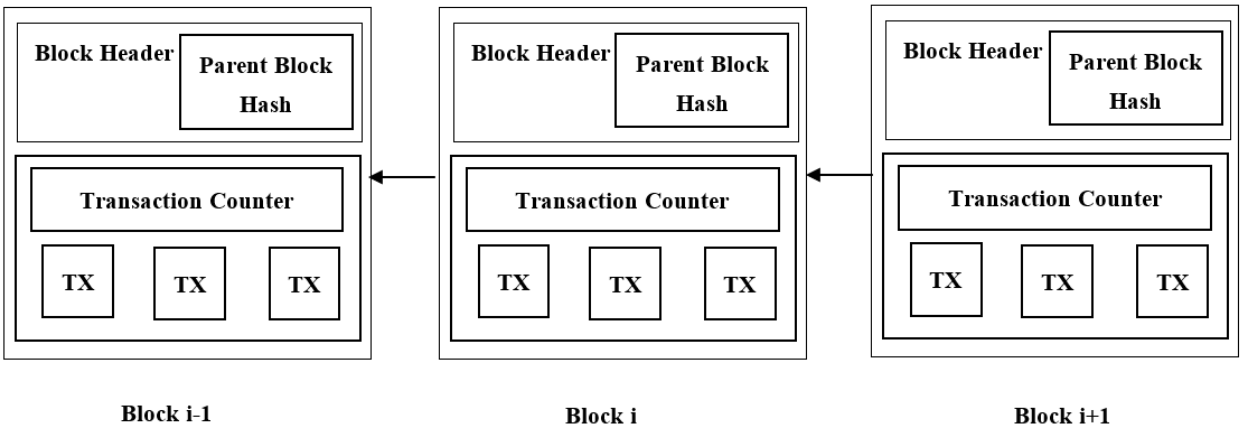

Figure 7. Blockchain structure.

Blockchain technology is a shared private/public database involving actions performed and distributed across blockchain agents. The BT differs from present information systems in four ways, namely decentralization, security, appropriateness, and smart execution [169]. As mentioned, blockchain is a relatively new technology, and today, in many ways, it helps us live with greater security and speed. Not much time has passed since the advent of this technology. This technology has attracted the attention of researchers and scholars in this short period. Given the importance of this issue and the wide range of applications, Table 4 summarizes the various applications of blockchain.

Table 4. Blockchain utilization.

NO	Application	Reference	Year
1	IoT security, blockchain and medical (IoMT)	[170]	2020
2	IoT security, blockchain and transportation	[171]	2021
3	IoT security, blockchain and military	[123]	2020
4	IoT security, blockchain and industry and manufacturing	[172]	2020
5	IoT security, blockchain and smart cities	[173]	2021
6	IoT security, blockchain and smart grids	[174]	2018
7	IoT security, blockchain and smart home	[175]	2019
8	IoT security, blockchain and agriculture	[176]	2019
9	IoT security, blockchain and supply chain	[177]	2020
10	IoT security, blockchain and education systems	[178]	2021
11	IoT security, blockchain and business	[179]	2018
12	IoT security, blockchain and banking systems	[180]	2020

Of course, the great potential of blockchain technology is not yet known, and it will take time to discover this. Therefore, this emerging technology, as with other technologies, has many advantages and disadvantages. Thus, this part of the present study examines the many advantages and disadvantages, summarized in Table 5 [181].

Table 5. Advantages and disadvantages of blockchain technology [130].

No	Advantages	Disadvantages
1	Decentralized network	High energy consumption
2	Transparency	The difficult process of integration
3	Trusty chain	The implementation's high costs
4	Unalterable and indestructible technology	The signature verification
5	Fast processing	Opportunity to split the chain

5. Conclusions and Future Work

The IoT and its IoMT application have introduced a variety of platforms for exchanging information, expanding its applications in numerous fields daily. As IoMT technology is in the development phase and has not matured enough, it presents security risks due to a lack of user knowledge, poor maintenance, and inadequate standards. Hackers and adversaries can easily control IoMT devices with weak security by using malware for ransom. Hackers can access an unencrypted IoMT device through unencrypted communication. This paper offered a comprehensive survey of IoT, IoT security, IoMT, and IoMT security challenges, solutions, and future trends from new perspectives, which are briefly described as follows:

(1) Presenting a comprehensive study of previous research related to IoT and security and their applications, including E-health, education, the supply chain, etc.
(2) Comparison of the research works collected regarding various criteria, such as year of publication, scientific journals, and the approach adopted in multiple tables and graphs. Considering the charts, the upward trend in privacy in cyberspace uses the IoMT.
(3) Determining an approach has attracted researchers' attention more than other approaches to creating privacy.

However, more research is needed to find the deep role of blockchain in IoT and IoMT, which can be a take-home for researchers. Although in the body of the paper, the roles of IoMT and AI security, as well as IoMT and blockchain, are mentioned, more investigation on this topic is needed to make it more fruitful; as such, it can be a good direction for researchers working on this topic.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Tang, Y.; Elhoseny, M. Computer network security evaluation simulation model based on neural network. *J. Intell. Fuzzy Syst.* **2019**, *37*, 3197–3204. [CrossRef]
2. Mostefa, B.; Abdelkader, G. A Survey of Wireless Sensor Network Security in the Context of Internet of Things. In Proceedings of the 2017 4th International Conference on Information and Communication Technologies for Disaster Management, Münster, Germany, 11–13 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8.
3. 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]
4. Alfandi, O.; Khanji, S.; Ahmad, L.; Khattak, A. A survey on boosting IoT security and privacy through Blockchain: Exploration, requirements, and open issues. *Clust. Comput.* **2021**, *24*, 37–55. [CrossRef]
5. Ashourian, M. An Improved Node Scheduling Scheme for Resilient Packet Ring Network. *Majlesi J. Electr. Eng.* **2015**, *9*, 43.
6. Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In *Internet of Things*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 123–149. [CrossRef]
7. Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. *Comput. Sci. Rev.* **2021**, *40*, 100389. [CrossRef]
8. Gheisari, M. *A Survey on Clustering Algorithms in Wireless Sensor Networks: Challenges, Research, and Trends*; International Computer Symposium (ICS): Tainan, Taiwan, 2020; pp. 294–299. [CrossRef]
9. Raza, A. A Novel Forwarding and Caching Scheme for Information-Centric Software-Defined Networks. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–8. [CrossRef]
10. Ahmad, R.; Alsmadi, I. Machine learning approaches to IoT security: A systematic literature review. *Internet Things* **2021**, *14*, 100365. [CrossRef]
11. Xu, L.D.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
12. Fatehi, N.; Shahhoseini, H. A Hybrid Algorithm for Evaluating Trust in Online Social Networks. In Proceedings of the 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 29–30 October 2020; pp. 158–162.

13. Rezaeiye, P.P. Agent programming with object oriented (C++). In Proceedings of the Electrical, Computer and Communication Technologies (ICECCT), 2017 Second International Conference, Tamil Nadu, India, 22–24 February 2017.
14. 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]
15. Kou, Z. A Study on k-Hyperideals in Ordered Semihyperrings. *Symmetry* **2023**, *15*, 240. [CrossRef]
16. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
17. Noor, F.; Sajid, A.; Shah, S.B.H.; Zaman, M.; Gheisari, M.; Mariappan, V. Bayesian estimation and prediction for Burr-Rayleigh mixture model using censored data. *Int. J. Commun. Syst.* **2019**, *32*, e4094. [CrossRef]
18. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
19. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1686–1721. [CrossRef]
20. Pacheco, J.; Satam, S.; Hariri, S. IoT Security Development Framework for Building Trustworthy Smart Car Services. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 237–242.
21. Wang, S.; Hou, Y.; Gao, F.; Ji, X. A Novel IoT Access Architecture for Vehicle Monitoring System. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 639–642.
22. Mukhopadhyay, D.; Gupta, M.; Attar, T.; Chavan, P.; Patel, V. An Attempt to Develop an Iot Based Vehicle Security System. In Proceedings of the 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Hyderabad, India, 17–19 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 195–198.
23. Girish, B.G.; Gowda, A.D.; Amreen, H.; Singh, K.A. IOT based security system for smart vehicle. *Int. Res. J. Eng. Technol.* **2018**, *5*, 2869–2874.
24. García-magariño, I.; Sendra, S.; Lacuesta, R.; Member, S. Security in vehicles with IoT by prioritization rules, vehicle certificates and trust management. *IEEE Internet Things J.* **2019**, *6*, 5927–5934. [CrossRef]
25. Sfar, A.R.; Challal, Y.; Moyal, P.; Natalizio, E. A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation. In *IEEE Transactions on Intelligent Transportation Systems*; IEEE: Piscataway, NJ, USA, 2020.
26. Hussain, M.M.; Alam, M.S.; Beg, M.S.; Ali, R. Searching for IoT Resources in Intelligent Transportation Cyberspace (T-CPS)—Requirements, Use-Cases and Security Aspects. In *Cybersecurity and Privacy in Cyber Physical Systems*; CRC Press: Boca Raton, FL, USA, 2019.
27. Lei, A.; Cao, Y.; Bao, S.; Asuquom, P.; Cruickshank, H.; Sun, Z. Blockchain-Based Dynamic Key Management for IoT-Transportation Security Protection. In *Blockchain for Distributed Systems Security*; Wiley: Hoboken, NJ, USA, 2019. [CrossRef]
28. Vinayaga-Sureshkanth, N. Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems. In Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security; Association for Computing Machinery: New York, NY, USA, 2020; pp. 31–35.
29. Zhang, J.; Wang, Y.; Li, S.; Shi, S. An Architecture for IoT-Enabled Smart Transportation Security System: A Geospatial Approach. *IEEE Internet Things J.* **2020**, *8*, 6205–6213. [CrossRef]
30. Priharti, W.; Sumaryo, S.; Saraswati, T.; Nurfadilah, M.R. IoT Based Logistics Vehicle Security Monitoring System. *IOP Conf. Ser. Mater. Sci. Eng. IOP Publ.* **2020**, *771*, 012012. [CrossRef]
31. Hammoudeh, M.; Epiphaniou, G.; Belguith, S.; Unal, D.; Adebisi, B.; Baker, T. A Service-Oriented Approach for Sensing in the Internet of Things: Intelligent Transportation Systems and Privacy Use Cases. *IEEE Sens. J.* **2020**, *21*, 15753–15761. [CrossRef]
32. Abbas, K.; Tawalbeh, L.A.A.; Rafiq, A.; Muthanna, A.; Elgendy, I.A.; El-Latif, A.; Ahmed, A. Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. *Secur. Commun. Netw.* **2021**, *2021*, 5597679. [CrossRef]
33. Masood, A.; Gupta, A. Enhanced Logistics Security Techniques Using IoT and 5G. In Proceedings of the 2020 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 4–6 August 2020; IEEE: New York, NY, USA, 2020; pp. 7–14.
34. Sergi, I.; Montanaro, T.; Benvenuto, F.L.; Patrono, L. A smart and secure logistics system based on IoT and cloud technologies. *Sensors* **2021**, *21*, 2231. [CrossRef]
35. Valera, A.J.J.; Zamora, M.A.; Skarmeta, A.F. An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environments. In Proceedings of the 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2010.
36. Tarouco, L.M.R.; Bertholdo, L.M.; Granville, L.Z.; Arbiza, L.M.R.; Carbone, F.; Marotta, M.; de Santanna, J.J.C. Internet of Things in Healthcare: Interoperatibility and Security Issues. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 6121–6125.
37. Liu, Y. CFDMA: A Novel Click Fraud Detection Method in Mobile Advertising. In Proceedings of the 2022 4th International Conference on Data Intelligence and Security (ICDIS), Shenzhen, China, 24–26 August 2022; pp. 394–401.
38. Kim, J.T. Privacy and security issues for healthcare system with embedded rfid system on Internet of things. *Adv. Sci. Technol. Lett.* **2014**, *72*, 109–112.

39. Woo, S.H. Medical Information Security and Standard Technology on IoT Environment. *J. Korean Inst. Inf. Commun. Eng.* **2015**, *19*, 2683–2688.
40. Gong, T.; Huang, H.; Li, P.; Jiang, H. A Medical Healthcare System for Privacy Protection Based on IoT. In Proceedings of the 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, China, 12–14 December 2015; pp. 217–222.
41. Alkeem, E.A.L.; Yeun, C.Y.; Zemerly, M.J. Security and Privacy Framework for Ubiquitous Healthcare IoT Devices. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 70–75.
42. Yaraziz, S.; Ahmad, J.; Mehdi, G.; Yang, L. Recent Trends towards Privacy-Preservation in Internet of Things, Its Challenges and Future Directions. *IET Circuits Devices Syst.* **2022**. [CrossRef]
43. Williams, P.A.H.; Mccauley, V. Always Connected: The Security Challenges of the Healthcare Internet of Things. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 30–35.
44. Bae, K.H.W. Proposing and verifying a security-enhanced protocol for IoT-based communication for medical devices. *Cluster Comput.* **2016**, *19*, 2335–2341.
45. Abouzakhar, N.S.; Jones, A.; Angelopoulou, O. Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017.
46. Wortman, P.A.; Tehranipoor, F.; Karimian, N.; Chandy, J.A. Proposing a Modeling Framework for Minimizing Security Vulnerabilities in IoT Systems in the Healthcare Domain. In Proceedings of the 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Orlando, FL, USA, 16–19 February 2017; pp. 185–188.
47. Acm, I.; Minoli, D. IoT Security (IoTSec) Mechanisms For e-Health and Ambient Assisted Living Applications. In Proceedings of the 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, USA, 17–19 July 2017.
48. Amir, J.; Mehdi, G.; Zhang, W.; Liu, Y.; Arun, K.S. An intelligent sustainable efficient transmission internet protocol to switch between User Datagram Protocol and Transmission Control Protocol in IoT computing. *Expert Syst.* **2022**, e13129. [CrossRef]
49. Alromaihi, S.; Elmedany, W. Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018.
50. Winnie, Y. Enhancing Data Security in Iot Healthcare Services Using Fog Computing. In Proceedings of the 2018 International Conference on Recent Trends in Advance Computing (ICRTAC), Chennai, India, 10–11 September 2018; pp. 200–205.
51. Alagar, V.; Alsaig, A.; Ormandjieva, O. Context-Based Security and Privacy for Healthcare IoT. In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, China, 17–19 August 2018.
52. Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1656–1665. [CrossRef]
53. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [CrossRef]
54. Hayakawa, T. Proposal and Application of Security/Safety Evaluation Method for Medical Device System that Includes IoT. In Proceedings of the 2018 VII International Conference on Network, Communication and Computing, Taipei City, Taiwan, 14–16 December 2018; pp. 157–164.
55. Martinez, J.B. Medical Device Security in the IoT Age. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, New York, NY, USA, 8–10 November 2018; pp. 128–134.
56. Yeole, A.; Kalbande, D.R.; Sharma, A. ScienceDirect ScienceDirect Security of 6LoWPAN IoT Networks in Hospitals for Medical Data Security of 6LoWPAN IoT Networks in Hospitals for Medical Data Exchange Exchange. *Procedia Comput. Sci.* **2019**, *152*, 212–221. [CrossRef]
57. Bradley, C.; El-tawab, S.; Heydari, M.H. Security Analysis of an IoT System Used for Indoor Localization in Healthcare Facilities. In Proceedings of the 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 27 April 2018; pp. 147–152.
58. Pirbhulal, S.; Pombo, N.; Felizardo, V.; Garcia, N.; Sodhro, A.H.; Mukhopadhyay, S.C. Towards Machine Learning Enabled Security Framework for IoT-Based Healthcare. In Proceedings of the 2019 13th International Conference on Sensing Technology (ICST), Sydney, Australia, 2–4 December 2019; pp. 13–18.
59. Yu, C.; Gheisari, M.; Liu, Y. A Lightweight Advertisement Ecosystem Simulation Platform for Security Analysis. In Proceedings of the 2022 6th International Conference on Cryptography, Security and Privacy (CSP), Tianjin, China, 14–16 January 2022; pp. 41–45. [CrossRef]
60. Fazeldehkordi, E.; Owe, O.; Noll, J. Security and Privacy in IoT Systems: A Case Study of Healthcare Products. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–8.
61. Yin, X.C.; Liu, Z.G.; Ndibanje, B.; Nkenyereye, L. An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks. *Sensors* **2019**, *19*, 3146. [CrossRef]

62. Salih, F.I.; Azaliah, N.; Bakar, A.; Hassan, N.H.; Yahya, F.; Kama, N. IOT Security Risk Management Model for Healthcare Industry. *Malays. J. Comput. Sci.* **2019**, 131–144. [CrossRef]
63. Verikoukis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT) Resolving the protection concerns for the novel circular economy bioinformatics. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 457–464.
64. Kamalov, F. Deep learning for Covid-19 forecasting: State-of-the-art review. *Neurocomputing* **2022**, *511*, 142–154. [CrossRef] [PubMed]
65. Alhat, S.; Bangal, N. Gaikwad, A. Khairnar, S. Enhancing Data Security in IoT Healthcare Services using Fog Computing. *Int. Res. J. Eng. Technol.* **2019**, *6*. [CrossRef]
66. Thirugnanam, R.S.M. Review of security challenges in healthcare internet of things. *Wirel. Netw.* **2020**, *27*, 5503–5509. [CrossRef]
67. Rahman, A.; Member, S.; Hossain, M.S.; Member, S.; Nabil, A. Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices. *IEEE Internet Things J.* **2020**, *8*, 9603–9610. [CrossRef]
68. Wazid, M.; Bera, B.; Mitra, A.; Das, A.; Ali, R. Private Blockchain-Envisioned Security Framework for AI-Enabled by Private Blockchain-Envisioned Security Framework for AI-Enabled IoT-Based Drone-Aided Healthcare Services. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 1–6.
69. Amoon, M.; Altameem, T.; Altameem, A. Internet of things Sensor Assisted Security and Quality Analysis for Health Care Data Sets Using Artificial Intelligent Based Heuristic Health Management System. *Measurement* **2020**, *161*, 107861. [CrossRef]
70. Nomikos, K.; Papadimitriou, A.; Stergiopoulos, G.; Koutras, D. On a Security-oriented Design Framework for Medical IoT. In Proceedings of the 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 26–28 August 2020; pp. 301–308.
71. Gopalan, S.S.; Raza, A.; Almobaideen, W. IoT Security in Healthcare using AI: A Survey. In Proceedings of the 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 16–18 March 2021.
72. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. *Comput. Commun.* **2020**, *166*, 154–164. [CrossRef]
73. Ghazal, T.M. Internet of Things with Artificial Intelligence for Health Care Security. *Arab. J. Sci. Eng.* **2021**, 0123456789. [CrossRef]
74. Oniani, S.; Marques, G.; Barnovi, S.; Pires, I.M.; Bhoi, A.K. *Artificial Intelligence for Internet of Things and Enhanced Medical Systems*; Springer: Singapore, 2021. [CrossRef]
75. Gheisari, M.; Javadpour, A.; Gao, J.; Abbasi, A.A.; Pham, Q.V.; Liu, Y. PPDMIT: A lightweight architecture for privacy-preserving data aggregation in the Internet of Things. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–13. [CrossRef]
76. Kharchenko, V.; Bardis, N. Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model. In Proceedings of the 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), Chania, Greece, 27–29 August 2016; pp. 313–318.
77. Kamalov, F.; Zgheib, R.; Leung, H.; Al-Gindy, A.; Moussa, S. Autoencoder-based Intrusion Detection System. In Proceedings of the 2021 International Conference on Engineering and Emerging Technologies (ICEET), Istanbul, Turkey, 27–28 October 2021; pp. 1–5. [CrossRef]
78. Chandrashekhar, K.G.; Karimi-Alaghehband, F.; Özgün, D. IoT Security Adoption into Business Processes: A Socio-Technical View. In Proceedings of the Americas Conference on Information Systems (AMCIS), Boston, MA, USA, 10–12 August 2017.
79. Bujari, A.; Furini, M.; Mandreoli, F.; Martoglia, R.; Montangero, M.; Ronzani, D. Standards, Security and Business Models: Key Challenges for the IoT Scenario. *Mob. Netw. Appl.* **2017**, *23*, 147–154. [CrossRef]
80. Yılmaz, H.E.; Sirel, A.; Esen, M.F. The Impact of Internet of Things Self-Security on Daily Business and Business Continuity. In *Handbook of Research on Cloud Computing and Big Data Applications in IoT*; IGI: Antwerp, Belgium, 2019; pp. 481–498. [CrossRef]
81. Rita, Z. Towards an ML-Based Semantic IoT for Pandemic Management: A Survey of Enabling Technologies for COVID-19. *Neurocomputing* **2023**, *528*, 160–177.
82. Moshayedi, A.J.; Roy, A.S.; Liao, L.; Lan, H.; Gheisari, M.; Abbasi, A.; Bamakan, S.M. Automation Attendance Systems Approaches: A Practical Review. *BOHR Int. J. Internet Things Artif. Intell. Mach. Learn.* **2021**, *1*, 23–31. [CrossRef]
83. Wrona, K. Securing the Internet of Things A Military Perspective. In Proceedings of the 2015 IEEE 2nd World Forum Internet Things (WF-IoT), Milan, Italy, 14–16 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 502–507.
84. Furtak, J.; Chudzikiewicz, J. Security Techniques for the WSN Link Layer within Military IoT. In Proceedings of the 2016 IEEE 3rd World Forum Internet Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 233–238.
85. Rao, Y.; Kosari, S.; Gheisari, M. New Results in Vague Incidence Graphs with Application. *J. Funct. Spaces* **2022**, *2022*, 3475536. [CrossRef]
86. Arafath, M.S.; Khan, K.; Sunitha, K.V.N. Incorporating privacy and security in military application based on opportunistic sensor network. *Int. J. Internet Technol. Secur. Trans.* **2017**, *7*, 295–316. [CrossRef]
87. Sfar, A.R.; Chtourou, Z.; Challal, Y. A Systemic and Cognitive Vision for IoT Security: A Case Study of Military Live Simulation and Security Challenges. In Proceedings of the 2017 International Conference on Smart, Monitored and Controlled Cities, Sfax, Tunisia, 17–19 February 2017; pp. 17–19.
88. Cha, S.; Baek, S.; Kang, S.; Kim, S. Security evaluation framework for military IoT devices. *Secur. Commun. Netw.* **2018**, *2018*, 6135845. [CrossRef]
89. Katalin, B. Possibilities and Security Challenges of Using Iot for Military Purposes. *Hadmérnök* **2018**, *13*, 378–390.

90. Pradhan, M.; Noll, J. Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems. *IEEE Commun. Mag.* **2020**, *58*, 14–20. [CrossRef]
91. Reidenberg, J.R.; Schaub, F. Achieving big data privacy in education. *Theory Res. Educ.* **2018**, *16*, 263–279. [CrossRef]
92. Toapanta, S.M.T.; López, J.M.V.; Soledispa, R.S.T.; Gallegos, L.E.M. Definition of a Security Prototype for IoT Applied to Higher Education. In Proceedings of the 2019 Third World Conf Smart Trends Syst Secur Sustain (WorldS4), London, UK, 30–31 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 115–120.
93. Badshah, A.; Ghani, A.; Qureshi, M.A. Smart Security Framework for Educational Institutions Using Internet of Things (IoT). *Comput. Mater. Contin.* **2019**, *61*, 81–101. [CrossRef]
94. Jones, K.M.; Asher, A.; Goben, A.; Perry, M.R.; Salo, D.; Briney, K.A.; Robertshaw, M.B. We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 1044–1059. [CrossRef]
95. ALEXEI, A. Analysis of IoT security issues used in Higher Education Institutions. *Int. J. Math. Comput. Res.* **2021**, *26*, 2277–2286.
96. Canbaz, M.A.; OHearon, K.; McKee, M.; Hossain, M.N. IoT Privacy and Security in Teaching Institutions: Inside the Classroom and Beyond. In Proceedings of the 2021 ASEE ASEE Virtual Annual Conference Content Access, Virtual Conference, 26 July 2021.
97. Yanambaka, V.P.; Mohanty, S.P. Making use of semiconductor manufacturing process variations: FinFET-based physical unclonable functions for efficient security integration in the IoT. *Analog Integr. Circuits Signal Process.* **2017**, *93*, 429–441. [CrossRef]
98. Toma, C.; Popa, M. IoT Security Approaches in Oil & Gas Solution Industry 4.0. *Inform. Econ.* **2018**, *22*, 46–61.
99. Shahbazi, Z.; Byun, Y.C. Integration of Blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors* **2021**, *21*, 1467. [CrossRef] [PubMed]
100. Bohli, J.M.; Skarmeta, A.; Moreno, M.V.; García, D.; Langendörfer, P. SMARTIE Project: Secure loT Data Management for Smart Cities. In Proceedings of the 2015 International Conference on Recent Advances in Internet of Things (RIoT 2015), Singapore, 7–9 April 2015; pp. 7–9.
101. Burange, A.W.; Misalkar, H.D. Review of Internet of Things in Development of Smart Cities with Data Management & Privacy. In Proceedings of the 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, 19–20 March 2015; pp. 189–195.
102. Li, W.; Song, H.; Member, S.; Zeng, F. Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities. *IEEE Internet Things J.* **2017**, *5*, 716–723. [CrossRef]
103. Latif, S.; Zafar, N.A. A Survey of Security and Privacy Issues in IoT for Smart Cities. In Proceedings of the 2017 Fifth International Conference on Aerospace Science & Engineering (ICASE), Islamabad, Pakistan, 14–16 November 2017; pp. 1–5.
104. Magaia, N.; Fonseca, R.; Muhammad, K.; Segundo, A.H.F.N.; Aloisio, V.; Neto, L.; de Albuquerque, V.H.C. Industrial Internet of Things Security enhanced with Deep Learning Approaches for Smart Cities. *IEEE Internet Things J.* **2020**, *8*, 6393–6405. [CrossRef]
105. Toma, C.; Alexandru, A.; Popa, M.; Zamfiroiu, A. IoT Solution for Smart Cities' Pollution Monitoring and the Security Challenges. *Sensors* **2019**, *19*, 3401. [CrossRef]
106. Shen, M.; Tang, X.; Zhu, L. Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE Internet Things J.* **2019**, *6*, 7702–7712. [CrossRef]
107. Al-Turjman, F.; Poncha, J. Intelligence, security, and vehicular sensor networks in Internet of things (IoT)-enabled smart-cities: An overview. *Comput. Electr. Eng.* **2020**, *87*, 106776. [CrossRef]
108. Chakrabarty, S. Secure Smart Cities Framework Using IoT and AI. In Proceedings of the 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dubai, United Arab Emirates, 12–16 December 2020.
109. Gheisari, M.; Mehdi, E. Data Storages in Wireless Sensor Networks to Deal with Disaster Management. In *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 655–682.
110. Kamalov, F.; Moussa, S.; Zgheib, R.; Mashaal, O. Feature Selection for Intrusion Detection Systems. In Proceedings of the 2020 13th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 12–13 December 2020; pp. 265–269. [CrossRef]
111. Janeera, D.A.; Gnanamalar, S.; Ramya, K.C.; Kumar, A.G. Internet of Things and Artificial Intelligence-Enabled Secure Autonomous Vehicles for Smart Cities. *Automot. Embed. Syst.* **2021**, 201–218. [CrossRef]
112. Lam, K.Y.; Mitra, S.; Gondesen, F.; Yi, X. Ant-centric iot security reference architecture–security-by-design for satellite-enabled smart cities. *IEEE Internet Things J.* **2022**, *9*, 5895–5908. [CrossRef]
113. Wang, Y.F.; Lin, W.M.; Zhang, T.; Ma, Y.Y. Research on Application and Security Protection of Internet of Things in Smart Grid. In Proceedings of the IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012), Shenzhen, China, 7–9 December 2012.
114. Sherburne, M.; Marchany, R.; Tront, J.; Tech, V. Implementing Moving Target IPv6 Defense to Secure 6LoWPAN in the Internet of Things and Smart Grid. In Proceedings of the 9th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 8–10 April 2014; pp. 37–40.
115. Bekara, C. Security Issues and Challenges for the IoT-based Smart Grid. *Procedia—Procedia Comput. Sci.* **2020**, *34*, 532–537. [CrossRef]
116. Chin, W.; Li, W.; Chen, H. Energy Big Data Security Threats in IoT-Based Smart Grid Communications. *IEEE Commun. Mag.* **2017**, *55*, 70–75. [CrossRef]
117. Guan, Z.; Li, J.; Wu, L.; Zhang, Y.; Wu, J.; Du, X. Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Smart Grid. *IEEE Internet Things J.* **2017**, *4*, 1934–1944. [CrossRef]

118. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
119. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. Security Aspects of Internet of Things aided Smart Grids: A Bibliometric Survey. *Internet Things* **2019**, *14*, 100111. [CrossRef]
120. Borgaonkar, R.; Jaatun, M.G.; Tøndel, I.A.; Degefa, M.Z. Improving smart grid security through 5G enabled IoT and edge computing. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6466. [CrossRef]
121. Saleem, A.; Khan, A.; Malik, S.U.R.; Pervaiz, H.; Malik, H.; Alam, M.; Jindal, A. FESDA: Fog-Enabled Secure Data Aggregation in Smart Grid IoT Network. *IEEE Internet Things J.* **2019**, *7*, 6132–6142. [CrossRef]
122. Baranwal, T.; Pateriya, P.K. Development of IoT Based Smart Security and Monitoring Devices for Agriculture. In Proceedings of the 2016 6th International Conference, Cloud System and Big Data Engineering (Confluence), Noida, India, 14–15 January 2016; pp. 597–602.
123. Mehdi, G.; Wang, G.; Chen, S.; Ali, S. A Method for Privacy-preserving in IoT-SDN Integration Environment. In Proceedings of the 16th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2018), Melbourne, Australia, 11–13 December 2018.
124. Balaji, V.R.; Prakash, N. IOT Based Smart Security and Monitoring Devices for Agriculture. *Int. J. Pure Appl. Math.* **2017**, *116*, 121–129.
125. Shabadi, L.S. Design and Implementation of IOT based Smart Security and Monitoring for Connected Smart Farming. *Int. J. Comput. Appl.* **2018**, *179*, 1–4.
126. Nithin, V.; Mishra, S.; Devarubiny, P.; Muthulakshmi, S. Iot Enabled Farming Assist and Security Using Machine Learning. *ARPN J. Eng. Appl. Sci.* **2019**, *14*, 1809–1819.
127. Gundu, T.; Maronga, V.L. IoT Security and Privacy: Turning on the Human Firewall in Smart Farming. In Proceedings of the 4th International Conference on the Internet, Cyber Security and Information Systems, Johannesburg, South Africa, 31 October–1 November 2019; pp. 95–104.
128. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on security threats in agricultural IoT and smart farming. *Sensors* **2020**, *20*, 6458. [CrossRef] [PubMed]
129. Ferrag, M.A.; Shu, L.E.I.; Member, S.; Yang, X. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
130. Vangala, A.; Das, A.K.; Member, S.; Kumar, N.; Member, S. Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective. *IEEE Sens J.* **2020**, *21*, 17591–17607. [CrossRef]
131. Saha, H.N.; Roy, R.; Chakraborty, M. Development of IoT-Based Smart Security and Monitoring Devices for Agriculture. In *Agricultural Informatics: Automation Using the IoT and Machine Learning*; Wiley: Hoboken, NJ, USA, 2021; pp. 147–169. Available online: https://doi.org/10.1002/9781119769231.ch8 (accessed on 13 November 2022).
132. Rosline, G.J.; Rani, P.; Gnana Rajesh, D. Comprehensive Analysis on Security Threats Prevalent in IoT-Based Smart Farming Systems. In *Ubiquitous Intelligent Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 185–194.
133. Sharma, S.; Mittal, P. IoT-Based Smart Security System for Agriculture Fields. In *Cyber Security and Digital Forensics*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 143–151. [CrossRef]
134. Natarajan, Y.; Srihari, K.; Dhiman, G.; Chandragandhi, S.; Gheisari, M.; Liu, Y.; Alharbi, H.F. An IoT and machine learning-based routing protocol for reconfigurable engineering application. *IET Commun.* **2021**, *16*, 464–475. [CrossRef]
135. Santoso, F.K.; Vun, N.C.H. Securing IoT for Smart Home System. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015; pp. 5–6.
136. Gupta, P.; Chhabra, J. IoT Based Smart Home Design Using Power and Security Management. In Proceedings of the 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, 3–5 February 2016; pp. 6–10.
137. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
138. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
139. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based Smart Home: Security Challenges, Security Requirements and Solutions. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 7–8.
140. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-fovino, I.; Steri, G.; Baldini, G. Security and Privacy Issues for an IoT based Smart Home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 1292–1297.
141. Marksteiner, S.; Exp, J. An Overview of Wireless IoT Protocol Security in the Smart Home Domain. In Proceedings of the 2017 Internet of Things Business Models, Users, and Networks, Copenhagen, Denmark, 23–24 November 2017; pp. 1–8.
142. Bastos, D.; Shackleton, M. Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT–2018, London, UK, 28–29 March 2018. [CrossRef]
143. Shouran, Z.; Ashari, A. Internet of Things (IoT) of Smart Home: Privacy and Security. *Int. J. Comput. Appl.* **2019**, *182*, 3–8. [CrossRef]

144. Hiromoto, R.E.; Haney, M.; Vakanski, A. A Secure Architecture for IoT with Supply Chain Risk Management. In Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 21–23 September 2017; pp. 431–435.
145. Omitola, T.; Wills, G. Towards mapping the security challenges of the Internet of Things (IoT) supply chain. *Procedia Comput. Sci.* **2018**, *126*, 441–450. [CrossRef]
146. Zhou, W.; Piramuthu, S. IoT security perspective of a flexible healthcare supply chain. *Inf. Technol. Manag.* **2017**, *19*, 141–153. [CrossRef]
147. Nandakumar, L. Privacy-Aware State Estimation Based on Obfuscated Transformation and Differential Privacy: With Applications to Smart Grids and Supply Chain Economics. Master's Thesis, TU Delft, Delft, The Netherlands, 2018.
148. Farooq, M.J.; Zhu, Q. IoT Supply Chain Security: Overview, Challenges, and the Road Ahead. *arXiv* **2019**, arXiv:1908.07828.
149. Safkhani, M.; Rostampour, S.; Bendavid, Y.; Bagheri, N. IoT in medical & pharmaceutical: Designing lightweight RFID security protocols for ensuring supply chain integrity. *Comput. Netw.* **2020**, *181*, 107558. [CrossRef]
150. Shahzad, A.; Zhang, K.; Gherbi, A. Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive Blockchain. *Sensors* **2020**, *20*, 3760. [CrossRef] [PubMed]
151. Khan, M.A. Challenges Facing the Application of IoT in Medicine and Healthcare. *Int. J. Comput. Inf. Manuf.* **2021**, *1*. [CrossRef]
152. Kannan, S.; Dhiman, G.; Natarajan, Y.; Sharma, A.; Mohanty, S.N.; Soni, M.; Easwaran, U.; Ghorbani, H.; Asheralieva, A.; Gheisari, M. Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with IoT-Based Bat Agents for Traffic Management. *Electronics* **2021**, *10*, 785. [CrossRef]
153. Moreno, H.B.R.; Ramírez, M.R.; Hurtado, C.; Lobato, B.Y.M. IoT in Medical Context: Applications, Diagnostics, and Health Care. In *Innovation in Medicine and Healthcare Systems, and Multimedia*; Springer: Singapore, 2019; pp. 253–259.
154. Alam, S.; Shuaib, M.; Ahmad, S.; Jayakody, D.N.K.; Muthanna, A.; Bharany, S.; Elgendy, I.A. Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration. *Sustainability* **2022**, *14*, 15312. [CrossRef]
155. Ullah, I.; Khan, M.A.; Alkhalifah, A.; Nordin, R.; Alsharif, M.H.; Alghtani, A.H.; Aly, A.A. A Multi-Message Multi-Receiver Signcryption Scheme with Edge Computing for Secure and Reliable Wireless Internet of Medical Things Communications. *Sustainability* **2021**, *13*, 13184. [CrossRef]
156. Chaganti, R.; Azrour, M.; Vinayakumar, R.; Naga, V.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. [CrossRef]
157. Rahmani, A.M.; Mirmahaleh, S.H. Flexible-Clustering Based on Application Priority to Improve IoMT Efficiency and Dependability. *Sustainability* **2022**, *14*, 10666. [CrossRef]
158. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017.
159. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019.
160. Gheisari, M.; Wang, G.; Chen, S. An Edge Computing-enhanced Internet of Things Framework for Privacy-preserving in Smart City. *Comput. Electr. Eng.* **2020**, *81*, 106504. [CrossRef]
161. Alzubi, J.A.; Movassagh, A.; Gheisari, M.; Najafabadi, H.E.; Abbasi, A.A.; Liu, Y.; Najafabadi, A.P. A Dynamic SDN-Based Privacy-Preserving Approach for Smart City Using Trust Technique. In Proceedings of the 2022 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), Bam, Iran, 2–4 March 2022; pp. 1–5. [CrossRef]
162. Kumar, Y.; Koul, A.; Sisodia, P.S.; Shafi, J.; Kavita, V.; Gheisari, M.; Davoodi, M.B. Heart Failure Detection Using Quantum-Enhanced Machine Learning and Traditional Machine Learning Techniques for Internet of Artificially Intelligent Medical Things. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1616725. [CrossRef]
163. Hameed, S.S.; Hassan, W.H.; Latiff, L.A.; Ghabban, F. A systematic review of security and privacy issues in the Internet of medical things; the role of machine learning approaches. *PeerJ Comput. Sci.* **2021**, *7*, e414. [CrossRef]
164. Awotunde, J.B.; Jimoh, R.G.; Folorunso, S.O.; Adeniyi, E.A.; Abiodun, K.M.; Banjo, O.O. *Privacy and Security Concerns in IoT-Based Healthcare Systems in the Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 105–134.
165. Hasan, M.K.; Ghazal, T.M.; Saeed, R.A.; Pandey, B.; Gohel, H.; Eshmawi, A.A.; Alkhassawneh, H.M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Commun.* **2022**, *16*, 421–432. [CrossRef]
166. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. *Sensors* **2022**, *22*, 5517. [CrossRef]
167. Papaioannou, M. A survey on security threats and countermeasures in Internet of medical things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
168. Munusamy, A.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Srirama, S.N.; Alex, L.T.; Khosravi, M.R. Edge-Centric Secure Service Provisioning in IoT-Enabled Maritime Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, 1–10. [CrossRef]
169. Liu, P.; Hendalinpour, A.; Hamzehlou, M.; Feylizadeh, M.R.; Razmi, J. No titidentify and rank the challenges of implementing sustainable supply chain blockchain technology using the bayesian best worst methodle. *Technol. Econ. Dev. Econ.* **2021**, *27*, 656–680. [CrossRef]

170. Rathee, G.; Sharma, A.; Saini, H.; Kumar, R.; Iqbal, R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimed Tools Appl.* **2020**, *79*, 9711–9733. [CrossRef]
171. Li, L. Research on TCP Performance Model and Transport Agent Architecture in Broadband Wireless Network. *Scalable Comput. Pract. Exp.* **2021**, *22*, 193–201. [CrossRef]
172. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*, 100081. [CrossRef]
173. Gheisari, M. *IoT-SDNPP: A Method for Privacy-Preserving in Smart City with Software Defined Networking*; Vaidya, J., Li, J., Eds.; Algorithms and Architectures for Parallel Processing. ICA3PP 2018. Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018; Volume 11337.
174. Kim, S.K.; Huh, J.H. A study on the improvement of smart grid security performance and blockchain smart grid perspective. *Energies* **2018**, *11*, 1973. [CrossRef]
175. Singh, S.; Ra, I.H.; Meng, W.; Kaur, M.; Cho, G.H. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *Int. J. Distrib Sens. Netw.* **2019**, *15*. [CrossRef]
176. Devi, M.S.; Suguna, R.; Joshi, A.S.; Bagate, R.A. Design of IoT Blockchain Based Smart Agriculture for Enlightening Safety and Security. In *ICETCE 2019: Emerging Technologies in Computer Engineering: Microservices in Big Data Analytics*; Springer: Singapore, 2019; pp. 7–19.
177. Gheisari, M.; Wang, G.; Bhuiyan, M.Z.A.; Zhang, W. MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT. In Proceedings of the 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference, Guangzhou, China, 12–15 December 2017.
178. Liang, X.; Shetty, S.; Tosh, D.K.; Zhao, J.; Li, D.; Liu, J. A reliable data provenance and privacy preservation architecture for business-driven cyber-physical systems using Blockchain. *Int. J. Inf. Secur. Priv.* **2018**, *12*, 68–81. [CrossRef]
179. Wang, H.; Ma, S.; Dai, H.-N.; Imran, M.; Wang, T. Blockchain-based Data Privacy Management with Nudge Theory in Open Banking. *Future Gener. Comput. Syst.* **2020**, *110*, 812–823. [CrossRef]
180. Golosova, J.; Romanovs, A. The Advantages and Disadvantages of the Blockchain Technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2018.
181. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of Blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]