Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6360553, 10 pages
https://doi.org/10.1155/2022/6360553

Review Article

IoT Security Review: A Case Study of IIoT, IoV, and Smart Home

Jinnan Ma, Xuekui Shangguan, and Ying Zhang

Shanxi Information Industry Technology Research Institute Co., Ltd, Taiyuan 030012, China

Correspondence should be addressed to Ying Zhang; 875481217@qq.com

Received 18 May 2022; Revised 17 July 2022; Accepted 25 July 2022; Published 21 August 2022

Academic Editor: Chao Zhang

The Internet of Things (IoT) acts as a tremendous network that is constructed by fusing diverse sensors. IoT can achieve the interconnection of individuals, things, and machines at any place and time and improve the function performance of network applications. However, the security of IoT has always been a major problem that may limit the application perspective of IoT technologies. Nowadays, industrial IOT (IIoT), Internet of vehicles (IoV), and smart home have become the three primary emerging perspectives of the current IoT studies, and it is necessary to systematically highlight the security analysis of these three types of scenarios. Hence, in this paper, guided by the three major IoT application scenarios, i.e., IIoT, IoV, and smart home, we sum up the development status of IoT security technologies, analyzed corresponding technical difficulties, and discussed several future outlook of challenges and development trends for the IoT technology.

1. Introduction

IoT generally refers to the use of diverse information sensors, radio wave identification technology, laser scanners, infrared sensors, global positioning system, and other equipment to realize actual acquisition of data that need to be interacted, connected, and recorded [1]. The data collected by IoT devices include diverse necessary information such as light, biology, heat, sound, electricity, chemistry, mechanics, and other position information. By connecting the above information to the Internet, one can achieve intelligent perception, identification, and management. The Internet of Things is an extension and expansion network based on the Internet. Through the traditional telecommunication network, the respectively addressed public physical objects are interconnected. Therefore, it is an important part of the emerging information technology [2]. Moreover, the extreme expansion and extension of the Internet is another typical revolution in the information industry after the emergence of computers and the Internet. Therefore, it is often named “Internet where everything is connected” and “The third wave of the world information industry” [3, 4]. As early as 1999, Ashton [5], from MIT Auto-ID Research Center, first put forward the notion of IoT when he studied the connection of radio frequency identification information to the Internet. On November 17, 2005, the International Telecommunication Union [6] published the “ITU Internet Report 2005: Internet of Things,” which formally put forward the notion of “Internet of Things.”

With the sound growth of IoT industries, it has gradually penetrated into all aspects of life [7]. IoT has effectively promoted the intelligent development of infrastructures and day-to-day life such as industries, transportation, homes, and cities, making limited resources more rationally allocated, and greatly improved the quality of human life [8, 9]. However, whereas IoT technologies bring convenience to people’s lives, some security concerns also appear. Security is the most concerned factor when enterprises consider deploying IoT systems, and most of them temporarily shelve their plans to deploy IoT because of these security concerns, which hinders the rising trend of IoT and has greatly affected the popularization and development of IoT [7]. Therefore, IoT will only enter the realistic outbreak stage after breaking through the bottleneck of this security issues. Thus, the development of security and privacy techniques plays a significant place in promoting IoT technologies [10].

In recent years, the three fields of IIoT security, IoV security [11], and smart home security are relatively popular and occupy a large market share. In light of the above analysis, security research in the field of IoT exists in the direction of IIoT, IoV, and smart home. Therefore, this paper will systematically sort out the security issues in these three fields, respectively. We briefly sum up the three aspects below.

1.1. The Security of IIoT. IIoT refers to the use of automated, interconnected sensors, devices, and machinery to drive operational efficiencies at an industrial scale. Many IIoT-related security issues can be traced back to a lack of basic security protections, such as exposed ports, outdated software applications, and shallow authentication. These vulnerabilities directly connect to the network and provide a breach for a saboteur to gain easy access to the entire system. IIoT systems usually combine information technology with operational technology which adds another layer of potential threats [12, 13].

1.2. The Security of IoV. IoV means the dynamic mobile communication system in which vehicles and roads, vehicles and vehicles, vehicles and individuals, and vehicles and sensing devices interact to achieve the communication between vehicles and public networks. At present, IoV has become a significant application scenario of IoT and 5G networks [11]. For IoV, how to prevent vehicle information from being modified and ensure the security and IoV data sharing is a major topic in the development of intelligent driving technologies. In light of the above analysis, ensuring the availability, reliability, real time, and comprehensiveness of data information has become a key study topic in this field [14].

1.3. The Security of Smart Home. Smart home means the comprehensive application of wireless network communication technologies and sensing technologies to furniture household appliances, and it is an important part of IoT and smart home. Security issues act as a key factor hindering the growth of the smart home industry as well [10]. Since smart home products collect a large amount of private data from family members, many homeowners are worried about network security loopholes in connected smart home devices. Therefore, a safe, stable, and reliable smart home information security technology is the focus of existing researches.

In light of the above analysis, there are many types of security researches in the IoT field, relevant problems are complex, and there are relatively few systematic summaries in this field [12]. Therefore, this paper focuses on the three fields of IIoT, IoV, and smart home and focuses on IoT in various scenarios and security issues.

The arrangement of the paper is listed below: Section 2 analyzes the security of IIoT, mainly including the application of hardware securities, data securities, and blockchain technologies. Section 3 introduces the application of data securities, blockchain technologies, and trust management technologies in the security of IoV. Section 4 illustrates the application of network securities, system securities, and blockchain technologies in the field of smart home. Conclusions and future research directions are summed up for these three areas in the last section. Moreover, the overall framework of this paper is listed in Figure 1.

2. The Security of IIoT

With the deep integration of industrialization and informatization, the interconnection of production control systems and production management systems within various enterprises is increasing nowadays, and the need to improve product qualities and operational efficiencies by accessing networks is stronger as well. As a result, IIoT was born that acts as a relevant degree of integration of the Internet and industrial systems, as well as advanced computing, analysis, and sensing technologies. IIoT integrates industrial monitoring systems, material transportation systems, industrial production systems, consumer feedback information systems, industrial management systems, etc. and guides industrial production and improves efficiency by means of the intelligent processing results of diverse data centers [13].

The continuous deepening of IIoT in manufacturing applications means that the networked devices at the factory equipment layer will realize automatic communication and will be closely connected with the market layer and factory management. However, increasingly networked industrial environments make industrial control systems, networked devices, and industrial clouds more vulnerable to attackers, leading to threats such as plant downtime and operational disruption. Therefore, modern smart factories urgently need to take measures from the system, software, hardware, and other levels to handle increasingly complex industrial network security threats [15]. In recent years, based on the frequent occurrence of industrial IoT security incidents, information and network security issues have become a major obstacle to the promotion and application of IIoT [16].

The architecture of IIoT is primarily separated into the perception layer, network layer, and application layer [16]. For the protection of perception layers, related information can be prevented from being obtained at the source, which makes the IoT system secure at the source. At this stage, the security risks faced by IIoT mainly include network data security threats, hardware equipment security risks, software system vulnerability risks, and IoT's own security risks [17–19]. This means to fundamentally break through the security bottleneck of IIoT is the primary challenge to the adoption of IIoT. Moreover, the framework of this section is shown in Figure 2.

2.1. IIoT Hardware Security. The growing number of IoT devices has increased the area of system attacks, and these devices often own vulnerabilities which are opaque to the user yet may be exploited. The hardware devices of IIoT require multifaceted protection of the system back-end and the device itself [20]. Enterprises often organize a hardware device department and a back-end department to jointly solve the security problems of IIoT.

The security risk of IIoT hardware equipment is the biggest problem facing the device layer for the basic operation of IIoT. This includes not only the growing number of new equipment, but also the need to support older industrial control systems [21]. The continuous growth of devices has greatly increased the risk of system intrusion. Some older

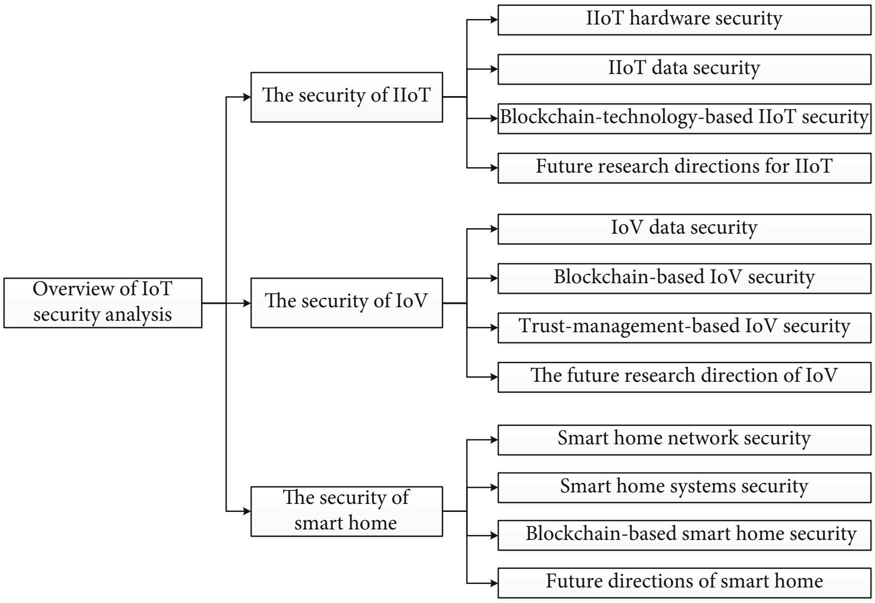
Overview of IoT security analysis
The security of IIoT
IIoT hardware security
IIoT data security
Blockchain-technology-based IIoT security
Future research directions for IIoT
The security of IoV
IoV data security
Blockchain-based IoV security
Trust-management-based IoV security
The future research direction of IoV
The security of smart home
Smart home network security
Smart home systems security
Blockchain-based smart home security
Future directions of smart home

Figure 1: Overall structure roadmap.

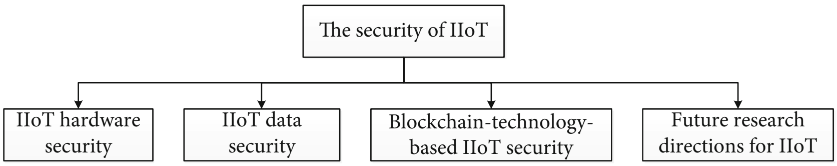
The security of IIoT
IIoT hardware security
IIoT data security
Blockchain-technology-based IIoT security
Future research directions for IIoT

Figure 2: Industrial IoT security research architecture.

devices that have weak computing and storage capabilities are easy to be attacked [22]. Moreover, some of the relevant literature is summarized as follows; please see Table 1.

2.2. IIoT Data Security. From the beginning, IIoT owns the characteristics of high interconnectivity, huge network scales, and higher risks than IoT. One of the biggest issues of IoT is to ensure the security of network, data, and devices. Protecting IIoT is a multifaceted work, and its security needs to be considered in all aspects [24].

A complete IIoT system has tens of thousands of "data nodes." Once a node is breached and infiltrated, the damage will spread through the node network at a high speed, which will have a big influence on the entire system. As of today, the IIoT field is full of risks from the perspective of information securities. Hackers often attack IIoT applications through system vulnerabilities to destroy the system or steal data [25]. Therefore, from the perspective of IIoT and industrial big data security issues, it is crucial to protect the network from the device layer where the data is generated. Data protection is a concern of the entire organization, and the more complex the network, the greater the need for data protection [26]. All in all, IIoT data security requires changes big and small to ensure that networks, systems, data, and devices are protected. Moreover, some of the relevant literature is summarized as follows, as shown in Table 2.

2.3. Blockchain Technology-Based IIoT Security. It is noticed that classical security technologies are not suitable for IoT since topology and resource constraints of IoT. Blockchain owns the feature of data traceability, decentralization, programmability, security, and trustworthiness and can provide new ideas for IoT security issues. The blockchain likes a database ledger, which can depict all transaction records, and the characteristics of completely saving all transaction records make it impossible for anyone to cheat. Simply put, the blockchain is a machine that creates trust, a safe and credible machine [28], which allows people who do not trust each other to exchange information safely without the coordination of an authoritative intermediate institution.

The blockchain system network is a classical P2P network with distributed heterogeneous features, whereas IIoT also has distributed characteristics. IIoT realizes information exchange by applying technologies such as intelligent perception and identification technology [26] and also meets operation requirements and the deployment of blockchain systems. The network features of the two ones determine that the IIoT can take the merits of the advantages of blockchain techniques to solve the pain points of IIoT.

Due to the integration of multiple systems, multiple platforms, and multiple devices, IIoT determines that it must coordinate the use of a variety of different data transmission methods and transmission protocols and open-related ports.

Table 1: Distribution papers in the field of IIoT hardware security.

Author	Title	Contributions
Lesjak et al. [20]	Hardware-security technologies for industrial IoT: TrustZone and security controller	Developed the TrustZone-based approach
Huberman [21]	Ensuring trust and security in the industrial IoT: the Internet of things (ubiquity symposium)	Presented a zero knowledge protocol
Basheer et al. [22]	Industrial-IoT-hardware security-improvement using plan load optimization method in cloud	Proposed the new system that is to deal with the manual arrival of more industrial defects
Yu et al. [23]	Toward data security in edge intelligent IIoT	Explored four key challenges in data security of edge intelligent IIoT, i.e., convenient usage, reliable storage, efficient search, and secure deletion

Table 2: Distribution papers in the field of IIoT data security.

Author	Title	Contributions
Lesjak et al. [24]	Security in industrial IoT-quo vadis?	Used a broker-based data exchange infrastructure and hardware-based security
Rajmohan and Srinivasan. [25]	Safety and security measurement in industrial environment based on smart IOT technology based augmented data recognizing scheme	Proposed a system design via employing the augmented data recognizing algorithm
Zahed et al. [26]	Content caching in industrial IoT: security and energy considerations	Explored the optimum location for the TCNs and found secured routes
Mosteiro-Sanchez et al. [27]	Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0	Presented an analysis of the most relevant security rules

At the same time, these factors make data vulnerable to threats during transmission [29]. Blockchain technology can provide a trusted, transparent, and secure communication channel for IIoT, enabling secure communication between devices. Through the decentralized verification system and consensus scheme of the blockchain, the intervention of illegal nodes can be avoided, and the transmitted data is processed by rigorous cryptography. Thus, the data security is guaranteed. Moreover, some of the relevant literature is summarized as follows; please see Table 3.

2.4. Future Research Directions for IIoT. Nowadays, there are still serious roadblocks from an IIoT security perspective. With the massive development of IIoT devices, the volume of generated data will also continue to increase, and whether the data is in edge computing, data centers, or cloud platforms, all data needs to be kept safe. Therefore, in the context of the IIoT, there will need to be a greater focus on how to protect equipment, data, communication, and processing power far beyond the traditional confines of IT [28, 29]. With the in-depth research of blockchain technology, the blockchain can be fully applied to IIoT in the future.

3. The Security of IoV

IoV technology acts as an exploration of IoT. The concept of IoV originated from the combination of VANET and IoT to improve the safety of road users and reduce the number of accidents. IoV integrates a brand-new generation of information with communication technologies and takes the moving vehicle as the information perception object [14]. Realize the network connection of people and vehicles and roads, and further realize the all-round network connection between vehicles and vehicles and vehicles and service platforms. The information transmission network structure of IoV can be divided into three layers from low to high, i.e., the perception layer, the transmission layer, and the application layer.

In recent years, the development of driverless cars and 5G technologies has enriched new fields, and IoV has gradually become the development trend of the automobile industry. Environmental feedback redefines people's understanding of traditional car travels. However, with the rapid development of smart cars, it also raises serious challenges to the security of the existing IoV [30]. Among them, network security and data security have become important scenarios for the sustainable growth of the IoV industry. With the continuous expansion of the commercial scale of IoV, if the transmission, collection, and use of relevant data are not effectively supervised and regulated, and the data is allowed to flow in an orderly manner, a great data security risk will be formed, and the personal information of vehicle users will be affected. Therefore, the privacy protection constitutes a clear threat. At the same time, the traditional centralized vehicle networking model and its reliance on third-party trust authority led to some security problems in the vehicle networking. If the centralized authority fails, the whole system may not work properly, reducing the availability of the system. Moreover, the framework of this section is shown in Figure 3.

3.1. IoV Data Security. IoV is an important field of deep integration of informatization and industrialization. With the growth of intelligent IoT technologies, the risks of IoV and

Table 3: Distribution papers in the field of blockchain technology-based IIoT security.

Author	Title	Contributions
Skwarek [28]	Blockchains as security-enabler for industrial IoT-applications	Presented application of general blockchain mechanisms
Wang et al. [29]	PoRX: a reputation incentive scheme for blockchain consensus of IIoT	Explored abnormal nodes in network collaboration

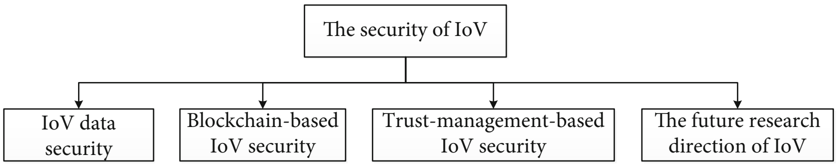
The security of IoV
IoV data security
Blockchain-based IoV security
Trust-management-based IoV security
The future research direction of IoV

Figure 3: IoV security research architecture.

data security have also become increasingly prominent. Whereas rapidly developing IoV technology, the United States and Europe attach great importance to the network security management, protection system construction, data security, and privacy protection of the IoV life cycle [30].

In the process of using smart cars, from data collection to transmission, to processing and use, there are network security and data security risks in the entire life cycle. Suppliers provide customized services to customers by collecting information about vehicles and personnel. For instance, more and more manufacturers use the biometric technology to collect data such as user's driving habits and usage preferences and use this data to mine and provide value-added services. Therefore, the data security and network security of IoV are also facing severe challenges. Once the database or control system is hacked through the network connection, it may lead to serious consequences such as personal fingerprints, iris, and other biometric information being stolen and driving routes and parameters being tampered with [31, 32]. Moreover, some of the relevant literature is summarized as follows, as shown in Table 4.

3.2. Blockchain-Based IoV Security. IoV technology requires secure and transparent systems. The blockchain owns the feature of nontampering, decentralization, and traceability, which can enhance the data privacy and security transparency of entire systems. Thus, the development of blockchain technologies can become an important boost to the data security of IoV [33]. The nontamperable modification of data by distributed storage of blockchain can permanently store each group of vehicles with location and time data, data related to the vehicle itself, and the corresponding owner information data and the owner's consumption habits, hobbies, and other information forever. Recorded in the blockchain, it can achieve the stabilization of automobile big data, solve the problems of vehicle data security and integrity [34], and improve the efficiency of collaborative management between government regulatory authorities and enterprises in the automotive industry.

The advantages of blockchain technologies and their applications to access control, communication security, and data security of IoV are of great significance to enhance the security of IoV. However, the blockchain-based IoV security technology still faces many challenges when showing its vitality. The inefficient block generation mechanism leads to high transaction data processing latency, the massive IoV data puts pressure on the storage space of blockchain nodes and the security risks of blockchain itself, the underlying technology of different blockchains restricts the interconnection between multiple chains, the anonymity of user identity of blockchain hinders the tracking and tracing of network security events, and the antitampering feature of blockchain increases the security of IoV and the difficulty of content management, etc., all urgently need to be addressed [35, 36]. Moreover, some of the relevant literature is summarized as follows; please see Table 5.

3.3. Trust Management-Based IoV Security. Trust is a key topic in IoV. Since the construction of IoV needs to simultaneously meet the large scale of data and the information sensitivity required by many services, it is a challenge to build a reliable IoV system. Trust is multifaceted and may include trust between users when automatically disseminating information and the trustworthiness of the IoT concept itself, etc. [37, 38] As IoT is decentralized, assessing its trustworthiness is very challenging. Therefore, minimizing the ambiguity of the service mode of IoV systems, clarifying the intention of information use, legally binding suppliers, and adopting the concept of privacy by design can improve the privacy security of users and promote establishment of the trust in IoV [39].

In existing privacy researches based on IoV, most of them have adopted the ideas of blockchain technologies, federated learning, hybrid trust management, node credibility evaluation and differential privacy [40], virtual travel itineraries, credibility and private information retrieval, etc. Moreover, some of the relevant literature is summarized as follows, as shown in Table 6.

3.4. The Future Research Direction of IoV. As there are enormous personal information exchanges and information recipients in IoV, it is extremely difficult to whole network

Table 4: Distribution papers in the field of IoV data security.

Author	Title	Contributions
Shariq et al. [30]	AnonSURP: an anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems	Designed an anonymous and secure RFID IoV protocol
Poomagal and Kumar. [31]	ECC based lightweight secure message conveyance protocol for satellite communication in Internet of vehicles (IoV)	Proposed rule for secure data correspondence between vehicular nodes in cities
Feng et al. [32]	Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV	Proposed a method that applicable to all ABE schemes with a tree access structure and can be applied to edge intelligent IoV

Table 5: Distribution papers in the field of blockchain-based IoV security.

Author	Title	Contributions
Wang et al. [33]	A novel IoV block-streaming service awareness and trusted verification scheme in 6G	Developed a trusted verification along with IoV block-streaming service awareness
Hu et al. [34]	A blockchain-based byzantine consensus algorithm for information authentication of the Internet of vehicles	Presented the byzantine consensus algorithm according to time sequence
Zhang et al. [35]	Blockchain-based asymmetric group key agreement protocol for Internet of vehicles	Proposed a blockchain-based asymmetric group key agreement protocol for IoV
Wang et al. [36]	A privacy enhancement scheme based on blockchain and blind signature for Internet of vehicles	Designed a vehicle privacy protection scheme in light of blind signature and blockchain

Table 6: Distribution papers in the field of trust management-based IoV security.

Author	Title	Contributions
Cinque et al. [37]	Blockchain-empowered decentralised trust management for the Internet of vehicles security	Explored suitable trust management for IoT and secure blockchain
Haddaji et al. [38]	Federated learning with blockchain approach for trust management in IoV	Proposed federated learning for trust management in IoV
Sohail et al. [39]	TrustWalker: An efficient trust assessment in vehicular Internet of things (VIoT) with security consideration	Presented a trust enhanced on-demand routing approach
Theodouli et al. [40]	Towards a blockchain-based identity and trust management framework for the IoV ecosystem	Developed a trust management framework and a blockchain-based identity

security, data security, and privacy security in the IoV industry. Future research on blockchain-based IoV security technology should also focus on client-oriented fine-grainedness [36], dynamic access control mechanisms, or cryptography-based communication protocols, from blockchain-based secure data transmission. Conduct in-depth research on distributed key distribution of communication protocols, lightweight consensus mechanism design, and blockchain-based car networking security architecture design.

4. The Security of Smart Home

With the enhancement of people's living standards, the concept of smart home has received more and more attention, and smart homes have gradually entered individuals' lives. The application of IoT in smart homes makes smart homes more convenient in terms of installation, operation, convenience, and use and improves the precision and digital intelligence of life technology services [41]. Bill Gates once said: "In the near future, a house without a smart home system will be like a house without Internet access today, which is not in line with the trend." Therefore, under the general trend of IoT, the family era has come.

However, high-level smart home security assistance is also a decisive factor for the rapid development of the smart home industry. Security issues in smart homes are usually not due to external intrusions (such as hacking) leading to malfunctions or device damage (such as malicious activation of the heating mode of the air conditioner in hot summer) [42]. From the application point of view, privacy leakage is the biggest security risk of the smart home. Current researches mainly focus on improving privacy security from the perspectives of network, system, and data processing. Moreover, the framework of this section is shown in Figure 4.

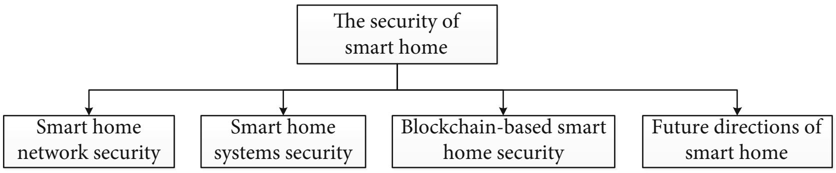
The security of smart home
Smart home network security
Smart home systems security
Blockchain-based smart home security
Future directions of smart home

FIGURE 4: Smart home security research architecture.

4.1. Smart Home Network Security. Cybersecurity has become a realistic issue in the growth of smart services. The smart home network system consists of three parts: terminal controller, IoT devices, and network [41]. The user sends commands to IoT devices, such as smart home appliances, through the network by downloading the corresponding client via using software and the Internet to achieve automatic control, remote control, and other functions [42].

As long as the home system is connected to the Internet, hackers will be able to invade the smart home system, so as to ensure the security of the smart home system first need to ensure network security, and the network entrance to the smart home is the home gateway. In reality, people often pay more attention to the stability of the gateway to access the network, ignoring the security of the gateway, and the only device with gateway commonly used in the home at present is only the router. Therefore, in the process of smart home applications, the privacy protection of family and individuals should be the primary issue [43]. Due to the fact that before the emergence of smart homes, both furniture and home appliances are silent and unconnected, the privacy of residential families and individuals would not have conditions and ways to be able to be accessed by third parties [41]. However with network connectivity, the smart home, a new type of system that can sense, network, store, compute, and execute, does make this possibility a reality.

In the application phase of smart home, the devices first have to access the cloud server by accessing the Internet and protocols. The most important of them are wireless IoT protocols, and the main ones are currently WiFi, Bluetooth, Zigbee, Z-Wave, and NB-IoT. The design flaws and security vulnerabilities of access protocols are also an important source of security threats to smart devices [42–44]. More seriously, because time-to-market is one of the key factors for a vendor's profitability, the security design and testing of devices by vendors is often far from adequate in order to be able to get to market as soon as possible. Moreover, some of the relevant literature is summarized as follows; please see Table 7.

4.2. Smart Home Systems Security. Smart home security requires a series of cybersecurity protocols or bills at the legal level but also needs measures at the technical level [45]. Smart homes are installed and deployed to indoor spaces as projects/systems, so the core remains the security of the system. It is ideal to design a smart home system with a reliable security policy and a well-defined system security and authentication process.

The connection of the network may expose the device to attackers inside or outside the network who can exploit software or hardware vulnerabilities to achieve. To solve this problem, the smart home domain monitoring system uses defensive programming, which monitors and checks whether the behavior of smart devices is safe and reasonable. In addition, many experts and scholars study the development of smart access control systems, smart door and window security systems, gas leak detection, personnel location, remote video surveillance, and database systems [46]. Such systems have the merits of low power consumption, low cost, distributed, and self-organization of wireless sensor networks, which can effectively improve the flexibility and reliability of security systems. Moreover, some of the relevant literature is summarized as follows; please see Table 8.

4.3. Blockchain-Based Smart Home Security. Security issues are a key factor hindering the growth of the smart home industry. As smart home products collect a large amount of privacy data of family members, many users are worried about the situation of network security vulnerability of the connected smart home devices. Blockchain technology can provide a solution to the smart home security problem, which can make device identification and identity verification more effective and reduce the possibility of malicious data tampering by others. The distributed network structure feature of blockchain can largely ensure that even if one or more nodes are breached, the data of the overall network system is still safe and secure [48–50]. Meanwhile, the integration of blockchain distributed technology with the underlying hardware makes it easier to design a secure consensus algorithm protocol, which makes the overall blockchain network operation more stable.

Applying blockchain technology in the data transmission of smart home devices can make the user's data and privacy more secure [49] and solve the security problem of smart home to some extent. Moreover, some of the relevant literature is summarized as follows, as shown in Table 9.

4.4. Future Directions of Smart Home. According to the security analysis from the perspectives of network protocols, data information, and platform systems in the smart home industry, the establishment of a unified standard system is the first task if the smart home industry wants to get a good and sustainable development [50]. At present, the security performance of smart home devices is still low, and the access data is still easy to be stolen or even tempered with. Therefore, device access control and protection of personal privacy data should also be considered in the future. Meanwhile, the capacity and processing speed of blockchain also need to be gradually improved so as to realize the extensive application

Table 7: Distribution papers in the field of smart home network security.

Author	Title	Contributions
Marksteiner et al. [41]	An overview of wireless IoT protocol security in the smart home domain	Presented an overview of IoT application domains
Robles and Kim [43]	A review on security in smart home development	Discussed smart home and security, reviewed the tool related to smart home security
Kim and Lee. [44]	Efficient and secure device clustering for networked home domains	Proposed a member list chain and member reputation-based association scheme

Table 8: Distribution papers in the field of smart home systems security.

Author	Title	Contributions
Bangali and Shaligram [42]	Design and implementation of security systems for smart home based on GSM technology	Suggested two methods for home security system, i.e., web camera and SMS with sensors, relays, and buzzers
Komninos et al. [45]	Survey in smart grid and smart home security: issues, challenges and countermeasures	The threats detected are categorized according to specific security goals set
Hu and Zhou [46]	The smart home security system based on wireless sensor network	Designed a smart home security system based on Zigbee wireless sensor networks
Kalofonos and Shakhshir [47]	Intuisec: a framework for intuitive user interaction with smart home security using mobile devices	Presented IntuiSec, a framework for intuitive user interaction

Table 9: Distribution papers in the field of blockchain-based smart home security.

Author	Title	Contributions
Khan et al. [48]	A machine learning approach for blockchain-based smart home networks security	Introduced a resource-efficient, blockchain-based solution for secure and private IoT
Ammi et al. [49]	Customized blockchain-based architecture for secure smart home for lightweight IoT	Explored a novel blockchain-based solution for secure smart home systems
Arif et al. [50]	Investigating smart home security: is blockchain the answer?	Described a secure smart home framework in light of consortium blockchain

of blockchain technology in the area of smart home securities [51].

5. Conclusions and Future Works

The promotion of IoT technologies needs to address plenty of related security issues and the large number of scenarios of IoT applications as well as the low generalization ability of security issues among scenarios which leads to the difficulty in the wide application of IoT technologies [50, 51]. Based on the security of IoT applications, researchers have actively started to explore this area and promote the rapid development of this field. In this work, we explore the security technologies for a total of three popular areas of IoT, i.e., IIoT, IoV, and smart home, and analyze them in the direction of device security, data security, network security, and system security. First, it is found that the application of blockchain technology has become an effective way to improve the security of IoT. Second, at the domain level, future research can also be done on coal, medical, and defense industries [52]. At the technical level, machine learning, deep learning, cloud computing, and big data techniques can be employed to further improve IoT security in the future. Finally, as IoT security research is the frontier of research direction in the field of IoT, more researchers are needed to conduct in-depth research in order to better exploit the value of IoT and in turn serve society [53, 54].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded in part by the Shanxi Province Scientific and Technological Achievements Transformation and Intellectual Property Transaction Service Platform Operation Services; the Shanxi Province Digital Economy Development Research Department; and the Information Technology Application Innovation Provincial Technology Innovation Center.

References

[1] P. Corcoran, "The Internet of Things: why now, and what's next?," *IEEE Consumer Electronics Magazine*, vol. 5, no. 1, pp. 63–68, 2016.

[2] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 58–67, 2011.

[3] I. Lee and K. Lee, "The Internet of Things (IoT): applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[4] C. M. Li, R. Wang, and L. Huang, "The key technology and application of the Internet of Things," *Applied Mechanics and Materials*, vol. 644-650, pp. 2812–2815, 2014.

[5] X. Feng, L. T. Yang, L. Wang, and A. Vinel, "Internet of things," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1101-1102, 2012.

[6] *ITU Internet Reports 2005: The Internet of Things*, vol. 1-28, International Telecommunication Union UIT, 2005.

[7] A. M. Rizwan, S. Wang, A. Z. Muhammad, J. A. Khan, A. Umair, and R. Salman, "Fog computing: an overview of big IoT data analytics," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7157192, 22 pages, 2018.

[8] C. Zhao, X. S. Li, and J. S. Chen, "Study on the application of internet of things in the logistics in forest industry," *Applied Mechanics and Materials*, vol. 97-98, pp. 664–668, 2011.

[9] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *2012 10th International Conference on Frontiers of Information Technology*, pp. 257–260, Islamabad, Pakistan, 2012.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, no. 15, pp. 146–164, 2015.

[11] L. Wu, J. Xu, L. Shi, and W. Zhou, "Optimize the communication cost of 5G internet of vehicles through coherent beamforming technology," *Wireless Communications and Mobile Computing*, vol. 2012, Article ID 6668984, 12 pages, 2021.

[12] N. Matsumoto, J. Fujita, H. Endoh, T. Yamada, K. Sawada, and O. Kaneko, "Asset management method of industrial IoT systems for cyber-security countermeasures," *Information*, vol. 12, no. 11, p. 460, 2021.

[13] S. Schneider, *The Industrial Internet of Things (IIoT): Applications and Taxonomy*, John Wiley and Sons, Inc, 2016.

[14] F. Wei, S. Zeadally, P. Vijayakumar, N. Kumar, and D. He, "An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3939–3951, 2021.

[15] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety*, vol. 139, pp. 156–178, 2015.

[16] Y. Li, Q. Cheng, and W. Shi, "Security analysis of a lightweight identity-based two-party authenticated key agreement protocol for IIoT environments," *Security and Communication Networks*, vol. 2021, Article ID 5573886, 6 pages, 2021.

[17] L. Ling, S. Li, and S. Zhao, "QoS-aware scheduling of services-oriented internet of things," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1497–1505, 2014.

[18] M. Brown, *Security: Using Static Analysis to Improve IIoT Device Security*, Panel Building and System Integration, 2017.

[19] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: a survey," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1667–1693, 2020.

[20] C. Lesjak, D. Hein, and J. Winter, "Hardware-security technologies for industrial IoT: TrustZone and security controller," in *IECON 2015-41st Annual Conference of the IEEE Industrial Electronics Society*, pp. 2589–2595, Yokohama, Japan, 2015.

[21] B. A. Huberman, "Ensuring trust and security in the industrial IoT: the Internet of things (Ubiquity symposium)," *Ubiquity*, vol. 2016, pp. 1–7, 2016.

[22] S. Basheer, M. Gopu, R. M. Mathew, M. A. Bivi, and M. Prabu, "Industrial-IoT-hardware security-improvement using plan load optimization method in cloud," *International Journal of Systems Assurance Engineering and Management*, vol. 6, pp. 1–8, 2021.

[23] Y. Yu, R. Chen, H. Li, Y. Li, and A. Tian, "Toward data security in edge intelligent IIoT," *IEEE Network*, vol. 33, no. 5, pp. 20–26, 2019.

[24] C. Lesjak, N. Druml, R. Matischek, T. Ruprechter, and G. Holweg, "Security in industrial IoT – quo vadis?," *Elektrotechnik und Informationstechnik*, vol. 133, no. 7, pp. 324–329, 2016.

[25] P. Rajmohan and P. S. S. Srinivasan, "Safety and security measurement in industrial environment based on smart IoT technology based augmented data recognizing scheme," *Computer Communications*, vol. 150, pp. 777–787, 2020.

[26] M. I. Aziz Zahed, I. Ahmad, D. Habibi, and Q. V. Phung, "Content caching in industrial IoT: security and energy considerations," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 491–504, 2020.

[27] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, "Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0," *Journal of Manufacturing Systems*, vol. 57, pp. 367–378, 2020.

[28] V. Skwarek, "Blockchains as security-enabler for industrial IoT-applications," *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, no. 3, pp. 301–311, 2017.

[29] E. K. Wang, Z. Liang, C. M. Chen, S. Kumari, and M. K. Khan, "PoRX: a reputation incentive scheme for blockchain consensus of IIoT," *Future Generation Computer Systems*, vol. 102, pp. 140–151, 2020.

[30] M. Shariq, K. Singh, P. K. Maurya, A. Ahmadian, and D. Taniar, "AnonSURP: an anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8577–8602, 2022.

[31] C. T. Poomagal and G. A. S. Kumar, "ECC based lightweight secure message conveyance protocol for satellite communication in internet of vehicles (IoV)," *Wireless Personal Communications*, vol. 113, no. 2, pp. 1359–1377, 2020.

[32] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13784–13795, 2020.

[33] Y. Wang, Y. Tian, X. Hei, L. Zhu, and W. Ji, "A novel IoV block-streaming service awareness and trusted verification scheme in 6G," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5197–5210, 2021.

[34] W. Hu, Y. Hu, W. Yao, and H. Li, “A blockchain-based byzantine consensus algorithm for information authentication of the Internet of vehicles,” *IEEE Access*, vol. 7, pp. 139703–139711, 2019.

[35] Q. Zhang, Y. Li, R. Wang et al., “Blockchain-based asymmetric group key agreement protocol for internet of vehicles,” *Computers and Electrical Engineering*, vol. 86, article 106713, 2020.

[36] H. Wang, J. Gan, Y. Feng, Y. Li, and X. Fu, “A privacy enhancement scheme based on blockchain and blind signature for Internet of vehicles,” *International Conference on Blockchain and Trustworthy Systems*, vol. 1490, pp. 368–387, 2021.

[37] M. Cinque, C. Esposito, S. Russo, and O. Tamburis, “Blockchain-empowered decentralised trust management for the Internet of Vehicles security,” *Computers and Electrical Engineering*, vol. 86, no. 12, article 106722, 2020.

[38] A. Haddaji, S. Ayed, and L. Chaari, “Federated learning with blockchain approach for trust management in IoV,” *AINA 2022: Advanced Information Networking and Applications*, vol. 449, pp. 411–423, 2022.

[39] M. Sohail, R. Ali, M. Kashif et al., “TrustWalker: an efficient trust assessment in vehicular Internet of things (VIoT) with security consideration,” *Sensors*, vol. 20, no. 14, p. 3945, 2020.

[40] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, “Towards a blockchain-based identity and trust management framework for the IoV ecosystem,” in *2020 Global Internet of Things Summit (GIoTS)*, pp. 1–6, Dublin, Ireland, 2020.

[41] S. Marksteiner, V. J. Exposito Jimenez, H. Valiant, and H. Zeiner, “An overview of wireless IoT protocol security in the smart home domain,” in *2017 Internet of Things Business Models, Users, and Networks*, Copenhagen, Denmark, 2017.

[42] J. Bangali and A. Shaligram, “Design and implementation of security systems for smart home based on GSM technology,” *International Journal of Smart Home*, vol. 7, no. 6, pp. 201–208, 2013.

[43] R. J. Robles and T. H. Kim, “A review on security in smart home development,” *International Journal of Advanced Science and Technology*, vol. 15, pp. 13–22, 2010.

[44] D. Kim and J. Lee, “Efficient and secure device clustering for networked home domains,” *IEEE Transactions on Consumer Electronics*, vol. 65, no. 2, pp. 224–232, 2019.

[45] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: issues, challenges and countermeasures,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[46] Y. Hu and T. Zhou, “The smart home security system based on wireless sensor network,” *Advanced Materials Research*, vol. 204-210, pp. 1490–1493, 2011.

[47] D. N. Kalofonos and S. Shakhshir, “Intuisec: a framework for intuitive user interaction with smart home security using mobile devices,” *Massachusetts Institute of Technology*, vol. 555, no. 4, pp. 659–708, 2008.

[48] M. A. Khan, S. Abbas, A. Rehman et al., “A machine learning approach for blockchain-based smart home networks security,” *IEEE Network*, vol. 35, no. 3, pp. 223–229, 2021.

[49] M. Ammi, S. Alarabi, and E. Benkhelifa, “Customized blockchain-based architecture for secure smart home for lightweight IoT,” *Information Processing and Management*, vol. 58, no. 3, article 102482, 2021.

[50] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, “Investigating smart home security: is blockchain the answer?,” *IEEE Access*, vol. 8, pp. 117802–117816, 2020.

[51] C. Chang, S. N. Srirama, and R. Buyya, “Mobile cloud business process management system for the internet of things: a survey,” *ACM Computing Surveys*, vol. 49, no. 4, pp. 1–42, 2017.

[52] Y. Zhao, M. Prabhu, and R. R. Ahmed, “Research trends and performance of IIoT communication network-architectural layers of petrochemical industry 4.0 for coping with circular economy,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8822786, 32 pages, 2021.

[53] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[54] D. Flores-Martin, J. Rojo, E. Moguel, J. Berrocal, and J. M. Murillo, “Smart nursing homes: self-management architecture based on IoT and machine learning for rural areas,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8874988, 15 pages, 2021.