Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9641143, 10 pages
https://doi.org/10.1155/2022/9641143

Review Article

The Development of Privacy Protection Standards for Smart Home

Donghang Liu,[1] **Chensi Wu**,[2] **Lulin Yang**,[2] **Xiaoying Zhao**,[2] **and Qifeng Sun**[2]

[1]*Shanxi Information Industry Technology Research Institute Co., Ltd, Taiyuan, China*
[2]*China Electronics Standardization Institute, Beijing, China*

Correspondence should be addressed to Chensi Wu; wucs@nipc.org.cn

Received 19 May 2022; Revised 26 June 2022; Accepted 6 July 2022; Published 22 July 2022

Academic Editor: Wentao Li

With the rapid development of network technology, society has entered the Internet of Things (IoT) era. Enriching IoT devices enable smart home privacy information to be easily obtained through data mining. Smart home privacy protection (SHPP) has a far-reaching impact on the development of all aspects of society. Industrial and academic circles pay great attention to the privacy protection of the smart home, and the ability to protect the privacy needs to be improved. SHPP standards are one way to evaluate privacy protection capabilities at this stage. Based on our research on privacy protection standards, this paper summarizes the development of privacy protection standards for the first time. It divides them into three phases: creation, exploration, and expansion. According to the characteristics of the privacy data rotation, the SHPP standard system is proposed, including basic commonality, critical technology, auxiliary management, test and certification, and device application. Finally, we focus on the opportunity and challenges of smart home privacy security standards brought by the current big data and prospect the trend of privacy protection technologies and standard study. They provide a connection for subsequent standard investigations.

1. Introduction

The Internet of Things (IoT) is becoming one of the most popular technologies, including sensor technology, intelligent technology, and network technology [1]. With the rapid development of the IoT technologies, IoT devices are integrated into people's daily life (brilliant homes, medical services, and others) [2]. A smart home connects various devices in the home through IoT technology, which can meet the living function and provide a comfortable, safe, efficient, and energy-saving living space with high humanization. IDC reported that compared with 2020, the global smart home device market increased by 11.7% in 2021, and the shipment volume exceeded 895 million units [3]. Smart home devices have proved their advantages during the worldwide pandemic. They add meaningful value to people's family life, such as alleviating social isolation, strengthening family safety, and providing convenience and entertainment. While optimizing people's lifestyle, smart home has also brought explosive growth of new data, which has become the hardest hit area for leaking personally identifiable information (PII) [4]. User privacy leaks frequently occur, the scale and impact of data leaks increase, and property losses are severe. For example, in March 2017, the smart toys under spiral toys leaked 2 million parents' and children's voice information. In December 2019, more than 4000 Amazon ring doorbell accounts were leaked, and hackers can realize remote monitoring, violate users' privacy, and steal important information. In January 2020, the details of about 2.4 million customers of Wyze, an intelligent security device company, were leaked, involving smart plugs, smart bulbs, and smart door locks. Thus, smart home privacy data protection has encountered severe challenges.

Protecting privacy is the practical need of human rights protection and the inevitable requirement of the development of information technology. Smart home privacy protection (SHPP) covers a wide range, involving every stage of the data life cycle (collection, use, retention, and disclosure) [5]. The smart home has prominent privacy characteristics, and the identification of private information depends on the specific application scenario. You can set the scenario mode by installing smart home devices with camera functions in indoor scenes such as living room and study. When you return home, the device will automatically be offline or dormant. The device will automatically turn on the guard mode when you leave home, which can protect the home's security through the intelligent home and detour the potential danger of privacy leakage caused by the device's excessive collection of private life information. Artificial intelligence technologies can extract PII from fine-grained data sets [6]. Finding the balance between intelligence and personal security has always been an essential topic for the smart home industry to explore and practice. Researchers have conducted much research on how to protect smart home privacy, made a series of progress, and put forward many mature privacy protection methods. Alshehri et al. [7] proposed a defense mechanism based on adding uniform random noise for defending against traffic analysis attacks. The process does not introduce excessive overhead. Literature [8] proposed an intelligent home privacy protection method that combines DES encryption and improves the secret algorithm's Least Significant Bit (LSB) information. This method provides dual protection for the secure transmission of smart home secret information, reducing the exposure of smart home personal information. The lack of understanding of the functions of smart home devices may cause information leakage. Literature [9] designed the incentive behavior framework to configure the intelligent home device with users.

There are limitations of approaches to solving privacy problems in different scenarios [10]. Different ways show some capability of privacy protection in smart homes. Measuring the size of privacy protection capability helps to understand the deficiencies. The SHPP standards are the method to qualitatively evaluate the privacy protection capability of smart homes. The achievements of privacy protection technology are solidified, promoted, and applied through standards, thereby promoting information technology progress to meet social needs better. The effective standardization of privacy is essential for mutual trust and cooperation between those related to developing big data interests. The value of SHPP standards can implement the importance of privacy protection, which is an effective path to prevent various types of privacy information security incidents [11]. Privacy protection standards can establish standards that follow together, promote legislation, and establish stable order. Scientific management of privacy promotes the reasonable use of data resources, maintains the balance of network ecology, safeguards the current and long-term interests of human society, guards the interests of consumers, and plays a significant role in protecting the people's body and property security.

There are still many deficiencies in the construction of SHPP standards. The standard formulation lacks overall coordination, and the perfect standard system has not yet been formed. The development of critical standards is slow and needs to be improved urgently. In the context of 5G networks, the convenience of the network will be more prominent, and more and more channels for privacy leakage will be. The acquisition of smart home privacy data becomes more superficial. Smart home standards help to better regulate the order of privacy protection in market competition. Many countries are promoting the establishment of international rules and regional personal information security mechanisms to cope with the crisis facing personal information in the era of big data [12]. Therefore, this paper takes the establishment of the standard system as the core and discusses the standard's development, challenges, and other issues. We hope that it can provide a reference for the research of SHPP standards to promote the formulation of SHPP standards. The contribution is summarized as follows.

(1) Sort out essential criteria for the protection of smart home privacy. Summarize the development process of SHPP standards and divide it into three stages in terms of time dimension: creation, exploration, and expansion. It helps people correctly understand the standard of privacy protection for smart homes

(2) According to the privacy life cycle's characteristics, the SHPP standard system framework is proposed, including fundamental commonality, key technologies, auxiliary management, testing and certification, and device application to provide a reference for subsequent technical standards

(3) Discuss the challenges of SHPP standards brought by the current big data, and look forward to some complex problems and possible solutions in privacy protection research

The structure of the paper is structured as follows: Section 2 introduces the development process of SHPP standards. Section 3 presents a system of SHPP standards. Section 4 gives challenges and opportunities for SHPP standards. Section 5 describes the direction of the SHPP research, and Section 6 concludes the paper.

2. Standard Development Stage

SHPP standards and norms are accompanied by people's awareness of privacy protection and the development of IoT technology. After more than 20 years, it has been continuously enriched, and privacy protection standards have provided solid cornerstones for studying SHPP standards. Based on the diversity of IoT and the complexity of privacy protection, this article sorts out the milestone nature of SHPP standards shown in Figure 1. With time, people have a clearer understanding of the development of SHPP standards. According to the awareness of personal protection and the diversity of privacy technologies, the construction of SHPP standards is divided into three main stages: creation, exploration, and expansion, which is the first time to summarize the development process of SHPP standards in terms of a time dimension.

2.1. Creation Stage. At the establishment of privacy protection standards, people mainly focus on privacy rights and have a preliminary understanding of the definition of

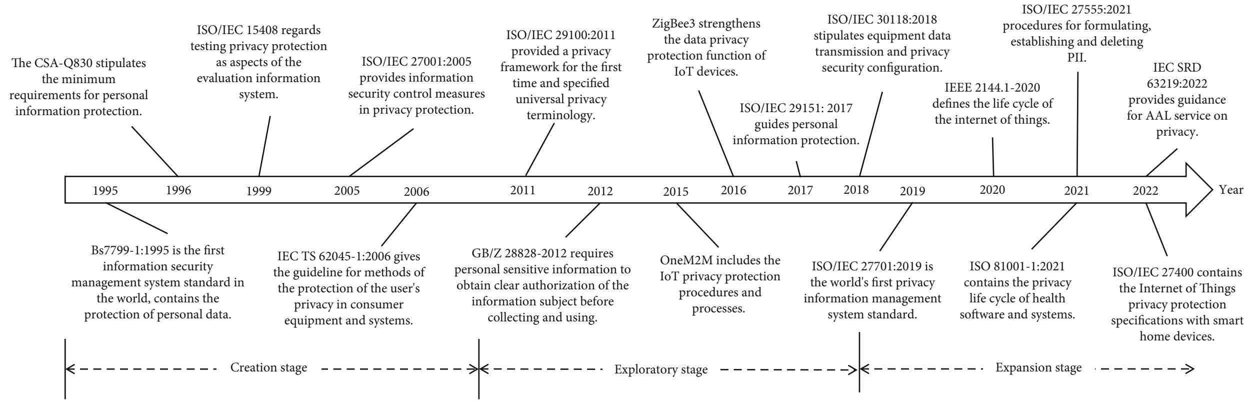
The CSA-Q830 stipulates the minimum requirements for personal information protection.
ISO/IEC 15408 regards testing privacy protection as aspects of the evaluation information system.
ISO/IEC 27001:2005 provides information security control measures in privacy protection.
ISO/IEC 29100:2011 provided a privacy framework for the first time and specified universal privacy terminology.
ZigBee3 strengthens the data privacy protection function of IoT devices.
ISO/IEC 29151: 2017 guides personal information protection.
ISO/IEC 30118:2018 stipulates equipment data transmission and privacy security configuration.
IEEE 2144.1-2020 defines the life cycle of the internet of things.
ISO/IEC 27555:2021 procedures for formulating, establishing and deleting PII.
IEC SRD 63219:2022 provides guidance for AAL service on privacy.
1995
1996
1999
2005
2006
2011
2012
2015
2016
2017
2018
2019
2020
2021
2022
Year
Bs7799-1:1995 is the first information security management system standard in the world, contains the protection of personal data.
IEC TS 62045-1:2006 gives the guideline for methods of the protection of the user's privacy in consumer equipment and systems.
GB/Z 28828-2012 requires personal sensitive information to obtain clear authorization of the information subject before collecting and using.
OneM2M includes the IoT privacy protection procedures and processes.
ISO/IEC 27701:2019 is the world's first privacy information management system standard.
ISO 81001-1:2021 contains the privacy life cycle of health software and systems.
ISO/IEC 27400 contains the Internet of Things privacy protection specifications with smart home devices.
Creation stage
Exploratory stage
Expansion stage

Figure 1: The development process of SHPP standards.

privacy existence and the connotation of privacy protection. The right to privacy emphasizes independence that individuals can be alone and restrict the violation of privacy. At this time, during the period of Ethernet, the overall concept of privacy protection was superficial. The standard development is slow, the substantive standards have fewer breakthroughs, and the implementation capacity of standards is weak. At this stage, privacy protection requirements mainly use the law as auxiliary means of self-discipline in various industries, uniformly regulating and protecting personal data privacy. The scope of application spreads from the government level to society.

Britain formulated Practice for Information Security Management (BS7799-1: 1995) is the world's first information security management system standard [13]. It first mentioned personal information and analyzed the scope and risks of data protection. After revision, it was equivalent to international standards in 2000 (ISO/IEC 17799: 2000) [14]. Countries such as Canada followed the development of privacy protection standards. CAN/CSA-Q830 made the public realize that personal information should be protected (https://www.csagroup.org/store/product/2700543/). The Q830 designed the principle of personal information management and put forward the minimum personal information protection requirements. To achieve a uniform concept, International Organization for Standardization (ISO) (https://www.iso.org/) and the International Electrotechnical Commission (IEC) (https://www.iec.ch/) issued ISO/IEC 15408 standard. This standard determined the privacy protection function, anonymous, pseudonym, liberation, and arbitrarily [15]. The bar is the international level that involves the content of privacy protection for the first time. Subsequently, ISO and IEC released several standards involving privacy. ISO/IEC 27001: 2005 pointed out the information security control measures required to protect the confidentiality and established an international consensus on personal data security management specifications. IEC TS 62045-1: 2006 gave consumers a guide to protecting user privacy when using the device [16].

2.2. Exploratory Stage. Government governance efficiency has gradually improved with the continuous emergence of new technologies. Society's requirements for privacy protection are becoming more and more abundant. More countries have begun to cooperate to explore privacy protection standards to refine the high-level principles and guidelines of privacy protection requirements. During the exploration stage, people have a deeper understanding of privacy protection. Focusing on IoT privacy protection standards, many countries and regions worldwide have released a series of standards that pay more attention to the substantial issues of privacy data processing. IoT privacy protection standards establish the foundation of SHPP standards. SHPP capabilities start to move toward dynamic and systematic.

The ISO/IEC Information Security Subtechnical Committee (ISO/IEC JTC 1/SC 27) has set up a working group responsible for studying identity management and privacy protection standards (WG5). WG5 proposed ISO/IEC 29100: 2011 standard gave 11 privacy principles for the first time, defining universal privacy terms, including PII, privacy violations, privacy control, and privacy strategies [17]. For PII, ISO/IEC 29151: 2017 to carry out personal identity information protection practice supports PII risk and influence evaluation [18]. China followed the pace of evolution and released the first personal information protection standard that guides personal information protection for public and commercial services (GB/Z 288282012) [19]. The most significant feature of the standard is that sensitive personal information must first obtain explicit user authorization before collecting and using.

The alliance's role in IoT privacy protection standards is becoming more and more prominent. Onem2m (machine to machine), founded by the European Telecommunications Standards Institute (ETSI), is the global community that develops IoT standards to enable interoperable, secure, and simple-to-deploy services for the IoT ecosystem (https://www.onem2m.org/). Onem2m standards adopted by the International Telecommunication Union (ITU) enclose various requirements, architectures, and protocols and have high robustness and scalability. The standards define IoT user data management framework and realize smart home privacy management based on this framework. ZigBee Alliance ignites creativity and collaboration in the IoT by developing, evolving, and promoting universal open standards that enable all objects to connect and interact securely (https://csaiot.org/). ZigBee3 is a wireless communication protocol designed by the ZigBee alliance with low power consumption, low latency, high reliability, and short distance. It is mainly suitable for wireless automatic control and can be embedded in various small devices: smart homes, smart cities, or other industries. ZigBee3 uses the symmetrical plus encryption algorithm to enforce the entire network, which further supports the data privacy protection of IoT devices [20].

2.3. Expansion Stage. Privacy protection has a large amount of essential work. The research of continuous in-depth IoT privacy protection technology has brought about the expansion of standard. The primary manifestation is that people have a deep understanding of privacy protection, and the awareness of privacy protection is more apparent. For example, if the user information is needed, the service provider should explicitly state the purpose, method, and scope of collecting and using the data. The user should enjoy the right to learn the truth while using data. At this stage, the number of standards has increased significantly, and the standardization of privacy protection management and technology has been comprehensively improved. The trend of the rational use of private information has become inertial and irreversible.

In recent years, international consensus has been more potent, and international standards that privacy protection can use have developed rapidly. ISO/IEC 30118: 2018 proposes to realize the core architecture, interfaces, protocols, and services of IoT and ecosystems and provides reference configuration for smart home device data transmission and privacy security [21]. ISO/IEC 27701: 2019 is the first international standard for privacy security management systems (PIMS) used for privacy control management. It provides richer content for smart home privacy collection and processing [22]. IEEE 2144.1-2020 standards define the IoT data management framework based on blockchain and build a smart home data life cycle (collection, processing, storage, analysis, use, exchange, and abandonment) [23].

In the context of big data, the characteristics of SHPP are becoming more evident, and protection measures are more professional and technical. SHPP's scope will continue to expand, and usage scenarios are becoming more and more specific. ISO 81001-1: 2021 standards involve the critical attributes of software and health systems in-home health device [24]. ISO/IEC 27400 puts forward a clear norm of privacy protection for intelligent home devices [25]. IEC SRD 63219: 2022 guides security, privacy, availability, and accessibility for home assistance device [26]. It is foreseeable that these are paved with the future privacy standards of smart homes.

2.4. Summarization of the Development. Standards are the most direct means of privacy data protection. Studying the progress of SHPP standards has theoretical and practical significance. SHPP standards have formed the momentum of globalization based on international, organizational, and national standards as the core. The implementation of international standards for privacy protection is conducive to promoting the progress of privacy technology and global economic exchanges and cooperation. The international standards of SHPP are constructed around the privacy security management system, privacy protection capabilities, and technical specifications of the PII principles. The international standards clarify the privacy framework's primary constituent elements and requirements. They guide the design, development, and implementation of privacy strategies and control and provide a high-level perspective for protecting personal information. Taking ISO as an example, the privacy standards in recent 20 years are counted, as shown in Figure 2. We can see the international consensus and vigorous development of privacy protection. Through continuous iteration standards, we can establish, implement, maintain, and improve privacy management capacity to reduce various risks of smart home data.

Although international standards realize and meet privacy protection requirements from different angles, they do not provide sufficient detailed guidance. The alliance standard complements this as the product of enterprise standardization activities. It is an effective tool for enterprise market competition with practicality, flexibility, and innovation. There are various types of alliance standards, which are closely combined with market demand, and alliance standards play an essential role in standardizing the market order.

The establishment of national SHPP standards is also a critical link. Each country's privacy protection circumstances are different, and the standards must connect with national development requirements. The American and European smart home standards cover great content and are in the world's leading position in privacy protection standards. In the future, privacy protection standards will absorb more power, privacy protection has become more stringent, and SHPP formulation has become more active.

3. SHPP Standard System

The standard system runs through all links of the privacy life cycle. We offer the standard composition framework based on the systematicness, hierarchy, integrity, and relevance from five aspects: basic common, critical technical, auxiliary management, testing and certification, and device application. The designed SHPP standard architecture is shown in Figure 3 [27].

The primary commonality standards of SHPP include terminology standards, reference framework standards, and guidelines criteria. The basic definition, framework, and suitable conditions are the critical point that supports the whole standard system. Term define concepts related to SHPP to clarify and define the scope of privacy protection. The reference architecture regulates the design of privacy collection, transmission, use, storage, and destruction, and it helps data managers to clarify the relationship between SHPP parts. The guidelines hold the applicability conditions of SHPP and determine whether privacy protection is needed. It guides and supervises the requirements that should be taken by data controllers, including function, performance, and consistency.

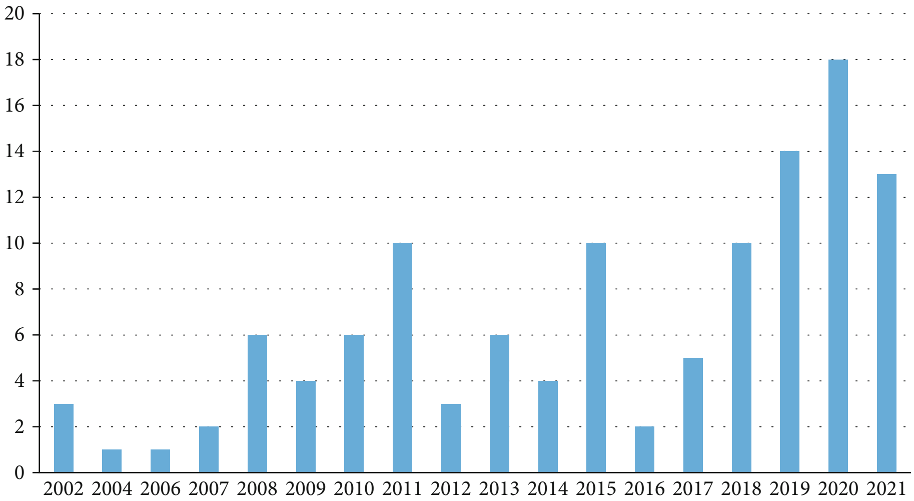

Figure 2: Statistics of standard number.

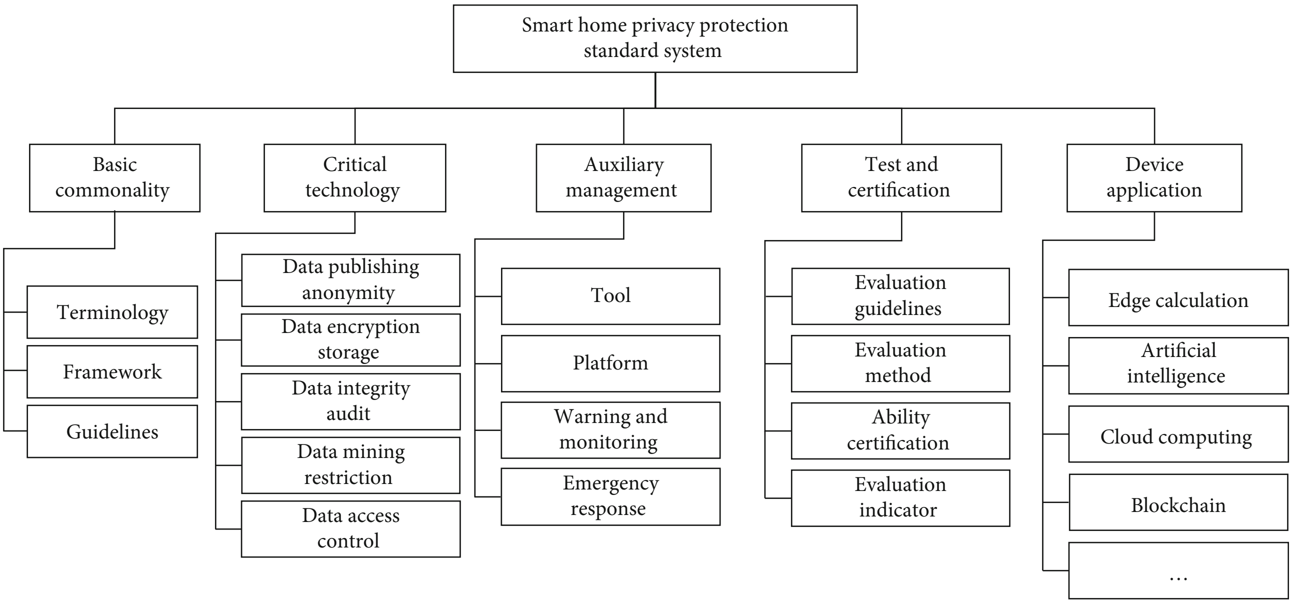

Figure 3: SHPP standard system.

Critical technologies play an essential and indispensable role in privacy protection that can guide the SHPP research and ensure the effectiveness of implementation. The vital technology standards include data publishing anonymity, data encryption storage, data integrity audit, data mining restriction, and data access control. Data publishing anonymity is used for data holders to hide specific user information when they publish data publicly to protect user privacy from disclosure [28]. Data encryption storage is aimed at the growing data privacy information and standardizing the computational overhead of encryption and decryption [29]. Data integrity audit checks frequent dynamic data operations, including tampering, discarding, and disclosing. Data mining restriction reduces the presentation of sensitive information. Data access control specifies the access control policy of data resources, such as user, resource, environment, and other attributes. No mature technology has been converted into standards, and there is still a long way to go before mature technologies are translated into standards. Therefore, people need to accelerate the pace of technology promotion and industrialization to improve the level of privacy management in technology.

The monitoring and early warning mechanism covers a wide range and are subject to various factors. Such standards are lacking. The auxiliary management standard includes four parts: tools, platform, early warning and monitoring, and emergency response, which are used to standardize the technical requirements of software and hardware tool platforms, such as function, performance, development, and integration, as well as the needs of daily early warning monitoring in the process of SHPP and emergency response after privacy disclosure. The tool is used to specify the technical conditions of software and hardware involved in SHPP, including function, performance, operating environment, secondary development, integration, use, and maintenance. The platform specifies the technical requirements, including operation, performance, working environment, interface, and integration. Early warning monitoring defines the analysis, prediction, and disposal processes and their technical requirements, including technical requirements and interface specifications. The standard can dynamically track privacy risks in real time according to the sensitivity and magnitude of privacy data. Emergency response is used to regulate the emergency response management and disposal measures of privacy security incidents, mainly including emergency strategies, disaster recovery backup, and recovery capabilities [30].

Test and certification standards include four parts: evaluation guidelines, evaluation methods, evaluation indicators, and ability certification, which are used to standardize the testing requirements and evaluation methods of SHPP. They can measure the degree of privacy protection and guide privacy managers to improve their security and service capabilities. The evaluation guidelines regulate the basic requirements of the testing and evaluation process, including the purpose, type, level, environment, and evaluation tools. The evaluation method specifies the technical requirements related to the privacy protection capability's test and evaluation process, including evaluation analysis, preparation, method selection, steps, and documents. Evaluation indicators specify the requirements of various indicators involved in SHPP capability testing and evaluation, such as stability, reliability, compliance, probability of privacy attribute disclosure, and block correlation [31]. Competency certification mainly handles the privacy protection level of an organization, product, service, and other related competency certification requirements, including privacy management competency certification and product privacy security certification.

Privacy protection needs to be consistent with the business. Device scenarios may set different goals for privacy protection, which need to be controlled by standards [32]. Device application standards for smart home device consider the differences in privacy data in different devices. According to different types of devices and various characteristics of business scenarios, the norms restrain the implementation of edge computing, blockchain, and other technologies [33] and guide the realization of personal protection requirements. For example, cloud computing may include cloud privacy security, terminal privacy collection, and guarantee capacity certification [34]. As the technical problems have not been completely solved, there are few standards in this field. The research is being carried out to eliminate the privacy risks and issues in the machine.

4. Challenges and Opportunities

Vast amounts of data have affected many aspects of people's lives. SHPP in IoT is an essential issue in big data security. With the increasing charge and complexity of privacy-related information, monitoring and protecting smart home privacy becomes more challenging [35]. At the same time, it is also necessary to recognize that technology cannot solve all problems. The deep integration of technologies has led to new methods, such as automation and intellectualization. These have created innovative thinking for SHPP, and new technologies provide new opportunities for standards.

4.1. Challenges

4.1.1. Privacy Risk Evaluation. Privacy risk evaluation identifies and mitigates the risk of privacy disclosure, which can be considered part of testing and certification in the standard system. By identifying possible privacy risks in smart homes and then quantifying these risks, we can deal with and prevent privacy protection problems in a proactive way [36]. Measuring the privacy risk can fully and intuitively understand the privacy protection strength of the current system. There are four privacy measurement methods based on anonymity, information entropy, set pair analysis theory, and differential privacy, each of which has its advantages, disadvantages, and scope of application [37]. The evaluation effect of privacy protection methods has not been unified, and there are no complete and universal measurement standards to guide the quantification of privacy protection intensity.

4.1.2. Weighing between Big Data and Privacy. With the growth of big data, information acquisition and privacy rights collide fiercely. In the discussion of big data and privacy, how to strengthen privacy protection and promote the development of big data has not yet been decided. To a certain extent, privacy protection will inevitably hinder data acquisition and restrict data use, thus delaying the application and development of big data. Data collection has created more and more possibilities to see user privacy, resulting in problems such as identification attacks, inaccurate data models, unfair use of sensitive information, high impact of personal behavior on the public, and large-scale data destruction [38]. The standard can be scientifically managed according to the development law of technology, and it is the first choice to rely on standards to balance the relationship between the two.

4.1.3. Demand Diversity. Each segment of smart homes has different needs for privacy protection. The privacy protection standards for specific application segments of smart homes are insufficient. For example, cloud computing has many intermediate data transmitting through the network, and the confidentiality of the data during the transmission process is threatened. In terms of user certification and access, the vast number of users also cause privacy risk. The scenes of contact with personal identity information are more diverse and flexible, bringing more attacks on PII [39].

4.1.4. Privacy Protection Methodology. There are still many gaps in the breadth and depth of privacy protection. Perfect SHPP methodology can better promote standardization work, including theoretical framework, privacy protection algorithm, and heterogeneous data processing. The earliest theoretical framework is Privacy by Design (PbD). PbD synthesizes the privacy design theory of technology, operating system, workflow, management structure, physical space, and infrastructure and integrates privacy protection into the overall design [40]. GDPR and ISO/IEC 27701 draw lessons from PbD theory, but the general law relationship, universality theory, and top-level design ability of privacy protection science still need to be strengthened.

4.1.5. Privacy Awareness. There is still a lack of awareness of privacy protection in society [41]. Governments and enterprises still leak their privacy and do not realize the seriousness of the problem. There is a view that when there are beneficiaries, accurate information should be published. In that way, there is a conflict between openness and transparency and privacy disclosure [42]. The essence of these situations is that the standards are not perfect enough, which leads to people's insufficient understanding of privacy protection. With the development of the economy and society, people's understanding of the importance of privacy protection is gradually strengthened. The establishment of privacy protection awareness and standards interact with each other. Through the adequate supervision and control of privacy by standards, the ability of privacy protection can develop on a healthy road. Privacy protection is integrated into society so that the standards can be effectively implemented.

4.2. Opportunities

4.2.1. The Urgency. Under the severe Internet security situation, big data has significantly changed privacy protection. In the process of using big data, there are some characteristics such as excessive data collection, massive useless data, inefficient analysis, and application of data. To successfully address privacy risks, it is urgent to further strengthen the protection of smart home privacy and formulate the comprehensive SHPP. Use data in a targeted and compliant manner and reduce the pressure of privacy protection. Rich standards in various scenes can further enhance the influence of norms.

4.2.2. The Necessity. Smart home privacy no longer stays in traditional privacy information such as name, ID number, bank card number, password, and family address. Interests, habits, behavior, and other information are becoming more and more common [43]. Once this data is abused or spread, it brings excellent instability to the society and even affects the country's security. Information protection has evolved particularly complicated. Therefore, improving privacy protection standards is more extensive in standardizing privacy acquisition and use, which also plays a good role in defining corresponding measures and responsibilities.

5. Prospects for Future Research

Privacy protection is always a critical direction of network security research. Through sorting out the above, the overall research status of the SHPP standard is as follows: the privacy protection model is still flawed, and a complete standard system has not yet been formed. There is a lack of objective and quantitative standards around the active protection of the entire privacy life cycle. Countries develop independently and have different goals. Some successful technical and management standards have been established for specific industries, but it is still difficult to cover a wide range. Therefore, the research on privacy protection needs to be further developed and improved. Table 1 summarizes some difficult problems and possible solutions in studying SHPP standards.

Search engines know users' browsing habits. Social tools understand what people are thinking [44]. The balance between data use and privacy protection is a vital issue. Privacy computing is a solution that considers both data value sharing and privacy protection, including secure multiparty computing, federated learning, a trusted execution environment, and other technologies. Standardized privacy computing can standardize the use of privacy data, improve the utilization of big data, and mine the value of big data without revealing user privacy to balance the relationship between data use and privacy protection [45]. At present, privacy computing theory and critical technology systems have a lot of work, but there are limitations in specific scenarios, which need standard guidance [46]. In the big data environment, data sources are diverse and dynamic. Even after anonymous data processing, users' privacy can still be analyzed [47]. Privacy protection technology for data mining is to study more appropriate data hiding technology and form standards to prevent privacy disclosure caused by data mining methods to improve the availability of big data as much as possible [48].

According to the characteristics of the smart home in different devices, the privacy protection standards with high requirements are constructed, and the privacy protection mechanism is integrated into the device design to improve the initiative of privacy protection. Improving privacy protection efficiency will help stimulate data processing capacity and achieve large-scale commercial landing. Privacy public chain can encrypt the input data, output data, and network status and conceal all nodes except the user himself, which provides a possible scheme for the efficiency of privacy protection [49].

Zero trust represents a new generation of network security protection, which means we do not trust anyone, devices, and systems inside or outside the enterprise network [50]. In the face of internal and external threats, the data security hierarchical dynamic access control is realized through the zero trust model to verify the data compliance. According to the data sensitivity, the manager monitors the data flow and locates the sensitive data at unknown locations [51]. Privacy measurement is aimed at measuring the degree of privacy protection, focusing on the evaluation index and measurement effect. It uses content identification technology to comprehensively evaluate the security status of privacy information and essential data. It timely removes privacy information and avoids gathering information excessively [52]. The irreversibility of privacy disclosure damage is enhanced, the difficulty of protection is upgraded, legislation to protect privacy lags, and it is easy to leave a back door. Unify the privacy protection mechanism and

Table 1: The problems and methods faced by SHPP research.

Questions	Methods
Quantitative balance between data usage and privacy protection	Privacy computing standardization
Data mining and privacy leakage	Data hiding technology
Privacy protection efficiency	Blockchain, privacy chain
Privacy measurement	Measurement system
Sensitive data access	Zero trust
Privacy protection mechanism	Active defense data compliance risk
Privacy protection methodology	New system and process
The field of privacy protection	Scene independence
Automated privacy compliance management	Automatic model

boost the privacy protection strategy iteratively to control the risk within a specific range.

SHPP has not yet formed a complete and systematic methodology. Privacy protection should not only start from the perspective of security technology but also breakthroughs from other social sciences such as economics, sociology, and ethics. Gradually expand the scope of SHPP, and establish a specific system or framework. The design or framework can guide the particular privacy protection work to reduce the possible loss caused by potential privacy risks. All smart home scenarios are developing the application of big data to obtain industry-specific data. Privacy standards for specific scenarios can manage privacy data more effectively [53]. Data compliance is closely related to each user. Individuals have differentiated privacy needs, and requirements vary by country and geography [54]. The standard can provide "customized" privacy-related services to each user through an automated approach and even help detect compliance requirements [55].

6. Conclusion

The smart home is a double-edged sword, conveying economic value while bringing privacy and security issues. The increase in privacy data has aroused people's sense of insecurity, and each person's different views and positions have led to the extension and continuous development of privacy issues. Information protection and rational use are always the themes of intelligent home privacy. The construction of SHPP standards has played practicality for clarifying the consensus of privacy protection and effectively enhancing the overall level of social privacy protection and also provides support for data security governance.

Based on sorting out the current status of the crucial privacy protection standards, this article summarizes the development process of SHPP standards. We divide it into three stages for the first time and analyze the construction of standards at each step in detail. The SHPP standard system is proposed to provide a reference for subsequent research, focusing on analyzing current data privacy security opportunities and challenges. Finally, the problems in the recent study are elaborated, and the future development direction is expected. Of course, this has certain deficiencies. The classification analysis of existing standards is insufficient, and the privacy protection capability that the standard can achieve is also not involved. We will explore each standard type in the follow-up work and focus on the technical details.

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 paper is supported by the Shanxi Province Digital Economy Development Research Department (No. 202104031402023), the Shanxi Province Scientific and Technological Achievements Transformation and Intellectual Property Transaction Service Platform Operation Services, Information Technology Application Innovation Provincial Technology Innovation Center (No. 202104010911033), the 2020 Industrial Technology Basic Public Service Platform Project of the Ministry of Industry and Information Technology, and the National key R & D Research (No. 2019YFB1405500).

References

[1] K. Kumar, A. Kumar, N. Kumar et al., "Dimensions of Internet of Things: technological taxonomy architecture applications and open challenges—a systematic review," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9148373, 23 pages, 2022.

[2] M. I. Alghamdi, "A hybrid model for intrusion detection in IoT applications," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 4553502, 9 pages, 2022.

[3] I. D. Corporation, *Worldwide quarterly smart home device tracker*, tech. rep., International Data Corporation, 2022.

[4] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *The Journal of Supercomputing*, vol. 77, no. 12, pp. 14053–14089, 2021.

[5] K. Rahul and R. K. Banyal, "Data life cycle management in big data analytics," *Procedia Computer Science*, vol. 173, pp. 364–371, 2020.

[6] J. Carmody, S. Shringarpure, and G. Venter, "AI and privacy concerns: a smart meter case study," *Journal of Information Communication and Ethics in Society*, vol. 19, no. 4, pp. 492–505, 2021.

[7] A. Alshehri, J. Granley, and C. Yue, "Attacking and protecting tunneled traffic of smart home devices," in *CODASPY'20: Tenth ACM Conference on Data and Application Security and Privacy*, pp. 259–270, New Orleans, LA, USA, Mrach 2020.

[8] L. Yang, H. Deng, R. P. Liu et al., "Smart home privacy protection based on the improved LSB information hiding," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 35, no. 12, 2021.

[9] J. Shams, N. A. G. Arachchilage, and J. M. Such, "Vision: why Johnny can't configure smart home? a behavioural framework for smart home privacy configuration," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 184–189, Genoa, Italy, September 2020.

[10] H. Jiang, Y. Gao, S. M. Sarwar, L. Garzaperez, and M. Robin, "Differential privacy in privacy-preserving big data and learning: challenge and opportunity," *Communications in Computer and Information Science*, vol. 1536, pp. 33–44, 2022.

[11] N. Fabiano, "Internet of Things and blockchain: legal issues and privacy. the challenge for a privacy standard," in *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)*, pp. 727–734, Exeter, UK, June 2017.

[12] X. Wang, W. Luo, X. Bai, and Y. Wang, "Research on big data security and privacy risk governance," in *2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR)*, pp. 15–18, Shanghai, China, November 2021.

[13] W. List, "Bs 7799 the code of practice for information security management," *The Computer Bulletin*, vol. 37, no. 6, pp. 8-9, 1995.

[14] C. Villarrubia, E. Fernández-Medina, and M. Piattini, "Analysis of ISO/IEC 17799: 2000 to be used in security metrics," in *International Conference on Security & Management*, Las Vegas, Nevada, USA, June 2007.

[15] A. Fiaschetti, V. Suraci, and F. D. Priscoli, "The shield framework: How to control security, privacy and dependability in complex systems," in *2012 Complexity in Engineering(COMPENG) Proceedings*, pp. 1–4, Aachen, Germany, June 2012.

[16] "Multimedia security-guideline for privacy protection of equipment and systems in and out of use-part 1: general," IEC TS 62045-1-2006, 2006.

[17] P. Sangaroonsilp, H. K. Dam, M. Choetkiertikul, C. Ragkhitwetsagul, and A. Ghose, "Mining and classifying privacy and data protection requirements in issue reports," CoRR, 2021, https://arxiv.org/abs/2112.13994.

[18] O. Drozd, "Privacy pattern catalogue: a tool for integrating privacy principles of ISO/IEC 29100 into the software development process," *International Federation for Information Processing*, vol. 476, pp. 129–140, 2016.

[19] X. Cui, X. Guo, and H. E. Ying, *The Evaluation and Analysis of Government Website's Privacy Policy in China:Based on the Investigation of 50 Government Websites*, Library Research, 2016.

[20] N. Shafqat, D. J. Dubois, D. Choffnes, A. Schulman, D. Bharadia, and A. Ranganathan, "Zleaks: Passive inference attacks on Zigbee based smart homes," CoRR, 2021, https://arxiv.org/abs/2107.10830.

[21] "Information technology—open connectivity foundation(OCF) specification — part 1: core specification," ISO/IEC 30118-1, 2018, https://www.iso.org/standard/53238.html.

[22] S. A. Grishaeva, "Development and implementation of privacy information management for compliance with international standard ISO 27701:2019," in *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies(IT&QM&IS)*, pp. 198–200, Yaroslavl, Russian Federation, September 2021.

[23] "IEEE draft standard for framework of blockchain-based Internet of Things(IoT) data management," P2144.1/D2, 2020.

[24] "Health software and health it systems safety, effectiveness and security — part 1: principles and concepts," ISO 81001-1, 2021, https://www.iso.org/standard/71538.html.

[25] "Cybersecurity—IoT security and privacy—guidelines," ISO/IEC, 2022, https://www.iso.org/standard/44373.html.

[26] "Active assisted living(AAL) system development guidance for AAL service providers," IEC SRD, 2022, https://webstore.iec.ch/publication/65370.

[27] F. Tao, X. Ma, T. Hu, Z. Huang, J. Cheng, and Q. Qinglin, "Research on digital twin standard system," *Computer Integrated Manufacturing Systems*, vol. 10, no. 25, pp. 2405–2418, 2019.

[28] J. Domingo-Ferrer, K. Muralidhar, and M. Bras-Amoros, "General confidentiality and utility metrics for privacy-preserving data publishing based on the permutation model," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2506–2517, 2021.

[29] B. A. Sassani (Sarrafpour), M. Alkorbi, N. Jamil, M. A. Naeem, and F. Mirza, "Evaluating encryption algorithms for sensitive data using different storage devices," *Scientific Programming*, vol. 2020, Article ID 6132312, 9 pages, 2020.

[30] X. Yang and A.'. Zhu, "Research on computer network security emergency response systematization," *Journal of Physics: Conference Series*, vol. 1771, no. 1, article 012012, 2021.

[31] Z. Li, W. Xu, H. Shi, Y. Zhang, and Y. Yan, "Security and privacy risk assessment of energy big data in cloud environment," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 2398460, 11 pages, 2021.

[32] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial iot, cyber threats, and standards landscape: evaluation and roadmap," *Sensors*, vol. 21, no. 11, p. 3901, 2021.

[33] J. Y. Dong, C. Song, T. Zhang, Y. Li, and H. Zheng, "Integration of edge computing and blockchain for provision of data fusion and secure big data analysis for Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9233267, 9 pages, 2022.

[34] X. Liu, "Towards blockchain-based resource allocation models for cloud-edge computing in IoT applications," *Wireless Personal Communications*, pp. 1–19, 2021.

[35] S. H. Ahmed and S. Zeebaree, "A survey on security and privacy challenges in smarthome based IoT," *International Journal of Contemporary Architecture*, vol. 8, no. 2, pp. 489–510, 2021.

[36] J. Chen, C. Wang, K. He et al., "Semantics-aware privacy risk assessment using self-learning weight assignment for mobile

apps," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 15–29, 2021.

[37] J. Xiong, M. S. Wang, Y. L. Tian, R. Ma, Z. Q. Yao, and M. W. Lin, "Research progress on privacy measurement for cloud data," *Journal of Software*, vol. 29, no. 7, pp. 1963–1980, 2018.

[38] A. Kaal, J. Klosek, and B. Waleski, "U.S. consumer privacy bill of rights: principles and impact," *Computer Law Review International*, vol. 13, no. 3, 2012.

[39] L. Yan, J. Yu, Y. Ye, H. Bai, J. Zhang, and J. Huang, "Multi-scene smart home system based on embedded chips," in *2017 IEEE International Conference on Mechatronics and Automation (ICMA)*, pp. 66–70, Takamatsu, Japan, August 2017.

[40] A. Cavoukian, "Understanding how to implement privacy by design, one step at a time," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 78–82, 2020.

[41] N. Gerber, B. Reinheimer, and M. Volkamer, "Home sweet home? investigating users' awareness of smart home privacy threats," in *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy(WSSP)*, p. 2018, Baltimore, MD, August 2018.

[42] L. Calloway, H. Hadan, S. Gopavaram, S. Mare, and L. J. Camp, "Privacy in crisis: participants' privacy preferences for health and marketing data during a pandemic," in *Proceedings of the 19th Workshop on Privacy in the Electronic Society*, New York, NY, SA, November 2020.

[43] Q. Liu, "Privacy protection technology based on machine learning and intelligent data recognition," *Security and Communication Networks*, vol. 2022, Article ID 1598826, 9 pages, 2022.

[44] G. Kapil, A. Agrawal, and R. A. Khan, "Big data security and privacy issues," *Asian Journal of Computer Science and Technology*, vol. 7, no. 2, pp. 128–132, 2018.

[45] B. Hou and R. Huang, "Enterprise privacy resource optimization and big data intelligent management strategy oriented to the Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 7280695, 10 pages, 2022.

[46] F. Li, H. Li, B. Niu, and J. J. Chen, "Privacy computing: concept, computing framework, and future development trends," *Engineering*, vol. 5, no. 6, pp. 1179–1192, 2019.

[47] M. L. Merani, D. Croce, and I. Tinnirello, "Rings for privacy: an architecture for large scale privacy-preserving data mining," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 6, pp. 1340–1352, 2021.

[48] H. W. Raj and S. Balachandran, "A survey of data anonymization techniques for privacy-preserving mining in bigdata," *Journal of Computer Science*, vol. 16, no. 2, pp. 194–201, 2020.

[49] O. Noam and O. Rottenstreich, "Realizing privacy aspects in blockchain networks," *Annals of Telecommunications*, vol. 77, no. 1-2, pp. 3–12, 2021.

[50] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting zero trust network architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, pp. 1309–1320, 2022.

[51] T. Viana, "Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture," *Applied Sciences*, vol. 11, no. 16, article 7499, 2021.

[52] X. F. Li, C. Zhao, and K. Tian, "Privacy measurement method using a graph structure on online social networks," *ETRI Journal*, vol. 43, no. 5, pp. 812–824, 2021.

[53] Y. Kim, D. Cho, and S. Hong, "Towards privacy-preserving domain adaptation," *IEEE Signal Processing Letters*, vol. 27, pp. 1675–1679, 2020.

[54] A. Qamar, T. Javed, and M. O. Beg, "Detecting compliance of privacy policies with data protection laws," CoRR, 2021, https://arxiv.org/abs/2102.12362.

[55] M. Farhadi, G. Pierre, and D. Miorandi, "Towards automated privacy compliance checking of applications in cloud and fog environments," in *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, Rome, Italy, August 2021.