Creativity and Innovation
2025, VOL. 9, NO. 2, 52-55
DOI: 10.47297/wspciWSP2516-252710.20250902

Privacy Information Security Protection of the Internet of Things in the Big Data Environment

Zishan Xie

South China Agricultural University, Guangzhou, China, 510604

ABSTRACT
With the deep integration of big data and the Internet of Things (IoT), IoT applications are becoming increasingly widespread. However, this has led to prominent privacy and information security issues. This paper analyzes the current situation, lists the harms caused by privacy breaches, and examines the reasons behind them. It also discusses research findings both domestically and internationally, explores the applicability and challenges of different technologies, and proposes various privacy protection solutions. The study shows that the comprehensive use of multiple technologies and strategies can enhance IoT privacy information security and ensure the healthy development of the IoT.

KEYWORDS
Component; Privacy Information Security Protection; Internet of Things; Big Data

1 Introduction

With the rapid development of technologies such as big data, information technology, wireless communication, and the internet, IoT technology has connected countless devices, sensors, and systems, creating an unprecedented intelligent world and ushering in the era of ubiquitous connectivity. However, with the explosive increase in IoT devices and the massive growth and flow of data, privacy breaches and data security issues have also emerged, becoming challenges we must face. Therefore, exploring how to formulate and implement effective privacy protection and data security strategies in the IoT environment is of great significance for maintaining the sustainable and healthy development of the IoT. Nowadays, both domestic and foreign countries attach increasing importance to privacy information protection, and related technologies are gradually maturing. Some scholars have achieved certain success in the research of related technologies and have explored their application scenarios in the IoT.

In the field of privacy information protection technologies, Zhang Tingting and others analyzed and processed different types of privacy data, established a differential attack game model, and calculated defense decision-making behaviors corresponding to transmission space integration based on probability. Their method for secure information transmission filters energy consumption, improves algorithmic defense efficiency, and offers relatively higher practical value [1]. Cao Zixiong and others embedded a differential privacy control algorithm into a federated large model. By implementing a dual privacy control mechanism at both the global and local levels, they enhanced the privacy protection capabilities of parameter fine-tuning based on federated learning and proposed that the next step of research would consider introducing additional pressures [2]. In the application of privacy protection technologies in the IoT, Richard K. Lomotey and others proposed a privacy-based IoT architecture that utilizes traceability technology [3]. This ensures that IoT data is only transmitted to nodes that have subscribed to receive the information. By leveraging traceability technology, they ensure high transparency, providing a digital audit trail. Multiple empirical evaluations were conducted in real-world wearable IoT ecosystems, demonstrating the superiority of the proposed work. Huang Yangyang introduced a security sharing method for IoT privacy data under attribute Logistic chaotic mapping [4]. A three-tier IoT privacy data security sharing model based on a master-slave structure was constructed, and a data access mechanism was designed to achieve IoT privacy data encryption with fewer operations and higher encryption strength.

By summarizing and comparing the methods of privacy information security protection for the IoT in the context of big data, this project can provide guidance for practical applications. It will promote the further improvement and innovation of privacy protection mechanisms, reduce the risk of personal privacy leakage in the IoT environment, and protect individuals' safety and rights. This will also enhance users' confidence in using IoT technologies.

2 Current Status of IoT Privacy Security in the Big Data Environment

Nowadays, the IoT has widely penetrated various fields of daily life and industrial production. In the area of smart homes, for example, Xiaomi's smart home ecosystem allows users to remotely control smart cameras, smart locks, and other devices through a smart speaker, greatly enhancing the convenience of daily life. In the industrial sector, Siemens factories use IoT technology to comprehensively digitize and monitor production processes, enabling predictive maintenance of equipment. This not only improves production efficiency but also reduces equipment failure rates. In smart city development, intelligent traffic management systems adjust traffic lights based on vehicle network technology, alleviating traffic congestion. Environmental monitoring collects data through IoT devices, providing a basis for environmental protection decisions.

However, as the IoT increasingly permeates people's daily lives, the issue of privacy and information security has become more severe. In 2023, a security vulnerability in the cameras of a well-known smart home brand led to the leakage of a large amount of family privacy. In 2022, a medical IoT company was hacked, and sensitive medical information of numerous patients was stolen. These incidents not only caused economic losses and emotional harm to users but also reduced their trust in IoT devices, hindered the promotion of IoT technology, and even raised the potential for a social trust crisis. The emergence of IoT privacy information security issues is mainly due to the following reasons: First, the number of IoT devices is huge and the types are complex. Some devices have insufficient security protection during the design and manufacturing process, with many security vulnerabilities. Second, during the data transmission process, some data is not encrypted or the encryption algorithm is not strong enough, making it easy to be stolen or tampered with. Third, IoT applications involve multiple links and many participants. There is a lack of standardization and effective supervision in data management and use, and there is a risk of data abuse and illegal acquisition.

3 Research Achievements on IoT Privacy Security in the Big Data Environment at Home and Abroad

3.1 Domestic Research Achievements

China has made significant achievements in the field of big data privacy and security, particularly standing out in algorithm innovation. Scholars have proposed innovative solutions to address complex privacy protection challenges, effectively tackling data security and privacy protection issues in scenarios such as the IoT and edge computing. At the same time, they are actively promoting the integration of emerging technologies with the IoT, utilizing cutting-edge technologies like blockchain and artificial intelligence to ensure the security of privacy data. However, there are also shortcomings in domestic research. Some technical algorithms are complex and have high demands on computing and storage resources, making them difficult to deploy and run on resource-constrained IoT devices. In the face of emerging technologies such as quantum computing, which pose challenges to traditional cryptography, related research is still in its early stages and requires further exploration.

3.2 Foreign Research Achievements

Foreign research focuses on the innovation of privacy protection mechanisms, providing new ideas for IoT privacy protection from multiple dimensions, such as dynamic sensor node clustering and the introduction of traceability technologies. Additionally, there is a strong emphasis on empirical research, with extensive real-world scenario experiments conducted to evaluate and verify the feasibility and effectiveness of technologies, driving the transformation of research outcomes into practical productivity. However, due to differences in the development environment, network architecture, and regulatory policies between domestic and foreign IoT settings, some foreign research outcomes require adaptive adjustments when applied domestically. Additionally, during the promotion of these results, challenges such as high implementation costs and significant device upgrade expenses may arise, limiting the expansion of their application scope.

4 Privacy Information Security Technologies in Different IoT Application Scenarios

4.1 Applicability Analysis of Different Privacy Information Security Technologies in the IoT

4.1.1 Edge Computing Data Security Protection Technology

In IoT scenarios with high real-time requirements, such as real-time monitoring of smart factory equipment and intelligent vehicle scheduling in smart transportation, edge computing data security protection technology has significant advantages. It can process data and protect privacy at the edge devices near the data source, reducing the risks of data transmission to the cloud and improving response speed. For example, Tesla's Gigafactory uses edge computing to process production line equipment operation data, ensuring production continuity and data security.

4.1.2 Blockchain Technology

In IoT scenarios involving multi-node data sharing and privacy protection, such as IoT supply chain management, blockchain technology offers significant advantages due to its decentralized distributed ledger system. Its immutability and traceability features ensure data sharing security. For example, in Walmart's food supply chain, consumers can trace the origin and other information of food products via blockchain, ensuring data security and integrity.

4.1.3 Location Privacy Protection Technology

In IoT scenarios such as intelligent transportation and logistics tracking that involve location information, location privacy protection technology is of great importance. It processes location information through means such as encryption and anonymization, such as using the k - anonymity technology. Cainiao Network uses this technology to encrypt the transportation location information of express parcels in the logistics industry, protecting users' privacy.

4.2 Challenges Faced During the Technology Application Process

4.2.1 Resource - Constrained IoT Devices

Most IoT devices, such as temperature and humidity sensor nodes, have limited computational power, storage capacity, and energy supply. Complex privacy protection algorithms, such as deep learning-based encryption algorithms, are difficult to run due to insufficient device resources, limiting the application of advanced privacy protection technologies.

4.2.2 Complex Network Environment

The IoT network consists of multiple communication protocols and architectures, with poor compatibility and interoperability and security vulnerabilities. Different protocols vary in data transmission rate, coverage, power consumption, and security mechanisms. Problems are likely to occur when data is transmitted across different networks, increasing the difficulty of implementing privacy protection technologies.

4.2.3 Lack of Standard Specifications

Currently, there is a lack of unified standards and regulations in the field of IoT privacy protection, making it difficult for products and technologies from different vendors to interoperate and work together. In the smart home sector, the privacy protection strategies and data formats of devices from different manufacturers vary, which increases development costs for companies and causes confusion for users.

5 Feasible Solutions for Privacy Information Protection in the IoT

5.1 Multi - Technology Integration Solution

Integrating blockchain technology, encryption technology, differential privacy technology, etc. can strengthen IoT privacy protection[5-7]. The blockchain ensures data integrity and source credibility, the encryption technology prevents data theft and leakage, and the differential privacy technology protects data security during data analysis and use.

5.2 Solution Based on Identity Authentication and Access Control

Establish a strict identity authentication mechanism, using multi - factor authentication, biometric identification, and other technologies to ensure the access of legitimate devices and users[8-9]. Implement fine - grained access control strategies, assigning access levels according to roles, permissions, and data sensitivity to reduce the risk of data leakage.

5.3 Dynamic Privacy Protection Solution

Adjust privacy protection strategies dynamically according to changes in IoT application scenarios and data sensitivity[10-11]. In the smart home scenario, when the user is at home, the privacy protection level of non - critical data can be reduced, and when the user is out, the protection can be strengthened.

5.4 Countermeasures to Avoid the Leakage of Customers' Privacy Information During IoT Information Transmission

Encrypt the transmitted data using high-strength encryption algorithms, such as AES and RSA[12]. Establish a secure transmission protocol, optimize existing protocols or use protocols specifically designed for the IoT to ensure data transmission security.

5.5 Countermeasures to Store Customers' Privacy Data Better to Avoid Leakage

Adopt a distributed storage method, dispersing data and storing it on multiple nodes, such as the Ceph and GlusterFS architectures[12]. Encrypt the stored data and use ciphertext index technology to achieve data retrieval and query, ensuring the privacy and security of data storage and use.

In conclusion, the protection of IoT privacy information requires the comprehensive application of multiple technologies and strategies, starting from multiple aspects to effectively enhance the security of privacy information in the IoT and promote the healthy development of the IoT.

References

[1] Zhang Tingting, Wang Zhiqiang. Simulation of network information security transmission based on privacy protection support[J]. Computer Simulation, 2024, 41(05):415-418+464.

[2] Cao Zixiong, Chen Yuxian, Jiang Xiumei. Application of Differential Privacy Technology Combined with Clustering Algorithm Based on Gaussian Kernel Function in Medical Data Security[J]. China Medical Devices, 2024, 39(07):28-35.

[3] Lomotey, R.K.; Sofranko, K.; Orji, R. Enhancing Privacy in Wearable IoT through a Provenance Architecture. Multimodal Technol. Interact. 2018, 2, 18. https://doi.org/10.3390/mti2020018

[4] Yangyang Huang. Secure sharing of IoT privacy data under attribute Logistic chaotic mapping[J]. Modern Electronics Technique, 2024, 47(13): 97-101. DOI: 10.16652/j.issn.1004-373x.2024.13.019.

[5] Jing Sun, Letian Sha, Ruchuan Wang, Fu Xiao, Wei Chen. "Leakage Perception Method for Backdoor Privacy in Industry Internet of Things Environment." Journal of Software 7(2018).

[6] Wei Yan, Mao Yanqin, Shen Subin. "A solution for data integrity verification based on blockchain." Computer Technology and Development, vol. 1, 2020.

[7] Nikolaos Zapoglou,Ioannis Patsakos,George Drosatos,Konstantinos Rantos. "Privacy-Preserving Blockchain-Based Solutions in the Internet of Things.".

[8] Priyanka More, Sachin Sakhare, Parikshit Mahalle. "Identity-Based Access Control in IoT: Enhancing Security through Mutual Cryptographic Authentication and Context Awareness.".

[9] Wu Liang, Li Liangqiang, Shao Peiji. "The Impact of Privacy Information Protection Strategies on Enterprise Decision-making Behavior in the Context of the Internet of Things." Systems Engineering 6 (2010).

[10] Xiaoshuang He, Hechuan Guo, Xueyu Cheng. "Blockchain-Based Privacy Protection Scheme for IoT-Assisted Educational Big Data Management." Wireless Communications and Mobile Computing(2021).

[11] Áine MacDermott, John Carr, Qi Shi, Mohd Rizuan Baharon, Gyu Myoung Lee. "Privacy-Preserving Dynamic Internet of Things (IoT).".

[12] Catarina Silva, J. Barraca. "Dynamic Delegation-based Privacy Preserving in IoT Architectures." 2022 9th International Conference on Future Internet of Things and Cloud (FiCloud)(2022).