Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5544716, 9 pages
https://doi.org/10.1155/2021/5544716

Research Article

Information Security Terminal Architecture of Power Transportation Mobile Internet of Things Based on Big Data Analysis

Xianzhi Tang[1] **and Chunyan Ding**[2]

[1]*College of Civil Engineering, Chongqing Vocational Institute of Engineering, Chongqing 402260, China*
[2]*Department of Mechanical Engineering, Yantai Engineering & Technology College, Yantai, 264006 Shandong, China*

Correspondence should be addressed to Chunyan Ding; dingchunyan@ytetc.edu.cn

Received 27 January 2021; Revised 16 March 2021; Accepted 27 April 2021; Published 22 May 2021

Academic Editor: Wenqing Wu

The progress of the social economy and the rapid development of the power field have created more favorable conditions for the construction of my country's power grid. In this network age, how to further realize the connection between the power system and the Internet of Things is the key content of many scholars' research. In the Internet of Things environment, there have been many excellent results in the collection, storage, and management of electric power big data, but the problem of information security has not been completely solved. Based on big data analysis and Internet of Things technology, this paper studies the architecture design of power information security terminals. In view of the diverse types of power grid mobile information and the large amount of data, this paper designs a power transportation mobile information security management system structure, which improves the effective management of power data by the system through big data, smart sensors, and wireless communication technology. According to the experiment, the power information security terminal constructed in this paper can effectively reduce communication resources and save communication costs in the process of aggregating multidimensional data. In the user satisfaction survey, residents' satisfaction with the convenience and safety of the intelligent power system is also as high as 9.312 and 9.233. On the whole, the application of big data and Internet of Things technology to the construction of power information security terminals can indeed improve the service efficiency of power companies under the premise of ensuring safety and allow users to have a better experience.

1. Introduction

Electricity plays a very important role in the country's economic development and people's daily life. Only by ensuring the stable operation of the power grid can the normal development of the entire society be guaranteed. The IoT is a network concept that realizes a wide range of connections between things and things, and between people and things through various information sensing devices such as radio frequency identification (RFID), infrared sensors, and global positioning systems (GPS). Its core technology is the identification and management of object information. In the field of power transportation, the most widely used value of Internet of Things technology is the collection, analysis, and management of power data in the power acquisition and control system. The main work of the power grid is to regulate and control the voltage and scientifically complete the transmission and distribution of electrical energy. Only by continuously improving the security of power information can the risks in the power communication process be effectively reduced.

In recent years, people have carried out a lot of research on the information security of the mobile Internet of Things, and the Internet of Things has become more and more widely used in various fields of life. Kok et al. has conducted research on smart grids embedded with renewable energy and distributed power generation. He believes that the development of public grids from the centralized control structure to decentralized control structure has changed rapidly. The

use of multiagent structure can help people further optimize the power control system. From the research results, further efforts are needed to improve the data islands in the smart grid [1]. Fadel et al. proposed a power system called smart grid (SG), which is used as an evolutionary system for power transformation, transmission, and distribution. SG uses renewable energy to generate electricity and manages the power system through smart meters and sensing and communication technologies. On the whole, this system has a good effect on improving performance, but there is still room for improvement in data security management [2]. Ejaz et al. analyzed the efficient energy management of the Internet of Things in smart cities. He believes that the Internet of Things provides many complex and diverse smart services for smart cities, and electric traffic management is a key example of implementing complex energy systems in smart cities. His team provided a unified framework for energy efficiency optimization and dispatching for IoT smart cities. However, this framework still lacks sufficient practicality for complex and changeable grid data [3].

My country's research on power information has been carried out earlier, and many good results have been achieved so far. Jia et al. conducted an analysis and research on the security of the power system. He believes that the successful development of smart grids is inseparable from the security of the system. He proposed a new and efficient safety analysis method, which includes a cascaded fault simulation module (CFSM) for postmortem analysis and a risk assessment module based on correlation neural network integration (DNNE). Although this method overcomes the problem of high computational cost in the traditional N-k algorithm, its stability needs long-term practice to be guaranteed [4]. Tu analyzed the interface design of the control and protection system based on the multiterminal HVDC flexible project. He took the control and protection system interface scheme of the multiterminal HVDC flexible project as an example and proved through research that the interface between the valve group controls satisfies the control protection system requirements. From the research report, the application of this scheme in power stations has a good protection effect on data security, but there is room for improvement in operating speed [5].

This article combines big data thinking and analyzes how to reasonably develop secure terminals for power transportation mobile information and form an Internet of Things system in the power industry. At the same time, this article introduces the Internet of Things information security technology and applies encryption algorithms to the development of Internet of Things security systems for power use. Smart grid is an inevitable trend of the development of the times, and the mobile Internet of Things security system for electric power transportation can effectively monitor the entire process of power transmission and distribution and conduct a more comprehensive management of power transportation [6].

2. Information Security Technology for Power Transportation Mobile Internet of Things

2.1. Basic Structure of Power Transportation Mobile Terminal. Electric power traffic data usually has the characteristics of many types, large data volume, and fast transmission speed. To realize the processing of electric power big data more effectively, the information security system must be improved [7]. In the construction of power information terminal, this article takes big data as the core concept to establish the connection between power data and users. To put it simply, you can refer to the operating idea of the Internet of Things, that is, using smart sensors to realize the mining, storage, and analysis of electric power data and finally realize the safe sharing of network information in the field of electric transportation and mobility [8]. Figure 1 is a schematic diagram of the power information security platform structure based on big data analysis.

It can be seen from Figure 1 that the power transportation mobile terminal system can be basically divided into a user layer, a big data analysis layer, and a terminal big data collection layer. There are three common service models for cloud computing, namely, infrastructure as a service, platform as a service, and software as a service [9, 10]. In this system, platform services and software services are mainly used to help users achieve various power data analysis requirements. The terminal collection layer uniformly collects the data generated during power operation through handheld or monitoring terminals. Generally speaking, the data involved in the power transportation mobile system includes but is not limited to power transformation, transmission, distribution data, line distribution data, and line operation data [11].

The big data analysis layer is the most complicated part of the system, and the data of the terminal collection layer will be stored here and received for further processing and scheduling [12]. Compared with the traditional data storage mode, big data storage has higher real-time performance, because the analysis layer will update the historical data in real time during data scheduling to ensure the dynamic allocation of data and ensure the smooth operation of the system.

2.2. Power Information Security Storage System Based on Big Data. According to the specific needs of data storage and analysis in electric transportation, this paper combines the basic structure of the cloud computing system to design a power information security storage system. This system consists of three parts, namely, storage, application, and management. In the safe storage system, a large amount of data information will be generated in the process of power transformation, transmission, and distribution, including static data, dynamic time series data, picture, and video data [13]. In order to ensure the smooth operation of transmission and distribution lines in complex environments, it is necessary to improve some of the problems in data storage and create more favorable conditions for data analysis and calculation [14].

2.3. Security Mechanism of the IoT Terminal System. The security architecture of the Internet of Things is usually divided into a perception layer, a network layer, and an application layer. The key difference between the security of the Internet of Things and the traditional network security lies in the perception of the security of the terminal system [15]. The Internet of Things terminal system is the forefront of the entire Internet of Things data perception and processing.

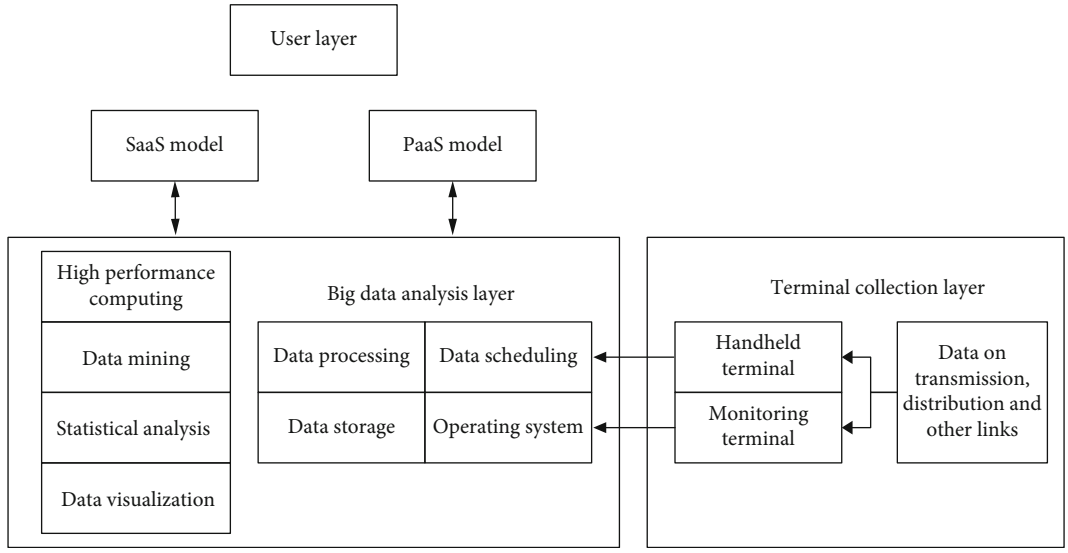

Figure 1: Structure diagram of power information security platform based on big data analysis.

Its biggest feature is limited resources. If you want to ensure the security of the Internet of Things, you must design a security mechanism that can adapt to the characteristics of the Internet of Things terminal system [16]. Generally speaking, RFID technology and wireless sensor network (WSN) technology are the most important technologies in the sensing layer.

2.3.1. RFID Technology. Radio frequency identification (RFID) is a kind of automatic identification technology. It carries out noncontact two-way data communication through radio frequency and uses radio frequency to read and write the recording media (electronic tags or radio frequency cards), so as to achieve the purpose of identifying targets and data exchange.

Radio frequency identification technology (RFID) is a noncontact two-way automatic data identification technology, because it has a strong data storage capacity, high accuracy and adaptability, and can simultaneously identify and process objects and tags. Its often used in the field of Internet of Things [17]. However, the openness of the RFID system will still cause it to have certain security problems. Although the existing security authentication protocols can detect the presence of false tags, these security authentication protocols are generally based on the single-proof interaction mode. Although this authentication mode is highly reliable, it cannot meet the actual needs of large-scale RFID systems in terms of efficiency [18].

2.3.2. Wireless Sensor Network (WSN) Technology. Wireless sensor network (WSN) is a distributed sensor network, combined with data fusion technology, and it has the effects of reducing node energy consumption, enhancing data perception capabilities, reducing network delay, and optimizing network resource allocation [19, 20]. Therefore, reasonable and efficient data fusion technology is very important for wireless sensor networks.

The data collected by a single node is limited, and the perception ability is limited. Therefore, it is necessary to deploy a large number of nodes in the wireless sensor network to improve the accuracy of the data and enhance the robustness of the network. However, nodes in the same detection area will have the phenomenon of communication crossing, resulting in data redundancy. If the node transmits redundant data directly to the sink, it will not only increase the amount of communication and calculation but also reduce the user's data decision-making ability [21]. Therefore, designing a reasonable and efficient data fusion technology, eliminating redundant data, and reducing computational complexity and node energy consumption, not only can improve the life cycle of the network but also improve the user's decision-making ability.

2.4. Mobile IoT Information Security Encryption Algorithm. The sensing layer lacks sufficient security protection barriers. If someone tries to attack the sensing nodes of the wireless sensor network, they will often start from the sensing layer. In addition, the sensing nodes in the sensing layer are distributed in various different complex environments, which further increase the probability of being attacked and causing information data damage and loss [22]. In order to ensure the confidentiality and integrity of the power, transportation, and mobile Internet of Things information, appropriate encryption algorithms must be used.

2.4.1. Byte Substitution. The round function of each round of the AES algorithm must go through the process of byte substitution, row shift, column mixing transformation, and round key addition operation. Compared with other algorithms, the AES algorithm is more symmetrical, and the expression is simple and easy to understand [23]. Byte substitution is the only nonlinear transformation in the algorithm. It is a bricker's replacement. The replacement contains an $s-$ box that acts on the state byte, denoted by SRD. Box $s-$ is a matrix of 16×16; so, there are 256 possible transformations. Among them, the algebra of byte substitution is

expressed as $bi, j = S[ai, j]$, and then the structure of SRD satisfies the formula:

$$\mathrm{SRD}[a] = f(g(a)). \tag{1}$$

If $g(a)$ represents transformation $a \to b$, then

$$a \to a^{-1} \mathrm{inGF}\left(2^8\right). \tag{2}$$

Among them, $f(a)$ is an affine transformation, and this change has no effect on nonlinearity, but it can make the algebraic expression very complicated.

2.4.2. Row Shift. The essence of the row shift is only one byte transformed; that is, the row in the state is cyclically shifted according to a different offset. For a 128*bits* component, the state offset is 0, 1, 2, and 3, and the offset used by each row can be any one of them [24]. The inverse operation of row shift is called InvShiftRows, which can make the rows of the state matrix cyclically shift. In the $AES - 128$ decryption algorithm, the first row moves three bytes to the right, and the second row moves two bytes to the right. The third row moves two bytes to the right, and the last row remains unchanged.

2.4.3. Column Confusion. Column confusion operation is a kind of linear transformation, which only performs mixing on each column included in the state. Column confusion transformation helps the state matrix to further provide higher diffusibility after row shifting and diffusion, which confuses each column of the state matrix [25]. This kind of replacement is to separately treat each column as a polynomial whose coefficients are in a finite field, then multiply with another intrinsic polynomial, and finally perform a modular operation on the formula $(x^4 + 1)$, where the mathematical formula of the polynomial $c(x)$ satisfies

$$c(x) = 0.3 \cdot x^3 + 0.1 \cdot x^2 + 0.1 \cdot x + 0.2. \tag{3}$$

When the inverse nematic hybrid transformation is expressed by matrix multiplication, the corresponding polynomial satisfies the formula:

$$\left(0.3 \cdot x^3 + 0.1 \cdot x^2 + 0.1 \cdot x + 0.2\right) \cdot d(x) = 0.1 \left(\mathrm{mod}\ x^4 + 1\right). \tag{4}$$

Among them, $d(x)$ satisfies

$$d(x) = 0B \cdot x^3 + 0D \cdot x^2 + 09 \cdot x + 0E. \tag{5}$$

2.4.4. Add Round Key. In the round key addition transformation, each round of the round transformation will have a round key, and the round key is expanded by the key, where ki, j is the round key, and the mathematical expression of round key addition is

$$bi, j = ai, j \oplus ki, j. \tag{6}$$

3. Construction Experiment of the Power Information Security System Based on Big Data Analysis

3.1. Experimental Background. The Internet of Things is the application of the Internet of Things in the smart grid. It is the result of the development of information and communication technology to a certain stage. It will effectively integrate the communication infrastructure resources and the power system infrastructure resources, improve the information level of the power system, and improve the current situation of the power system. With infrastructure utilization efficiency, it provides important technical support for power grid generation, transmission, transformation, distribution, and power consumption. A huge intelligent complex network integrates electrical equipment and facilities for unified management. Power information is not only diverse in types, large in data volume, and extremely fast in updating, it is difficult for traditional management methods to fully control power big data. During the preanalysis of the experiment, this article believes that the difficulty of the experiment will appear in the construction of the big data platform and the efficiency of part of the real-time information return. Therefore, this article focuses on information security and constructs the Internet of Things information system framework in the power field. In this way, the effect of comprehensive management of electric power big data can be improved.

3.2. Experiment Process. This article combines the characteristics of the power industry with big data and uses the radio frequency identification technology and intelligent information sensors in the Internet of Things to try to combine big data and the Internet of Things technology to construct a power information security terminal. The entire system is composed of the user layer, the big data analysis layer, and the terminal collection layer. The three are connected and complementary to each other, converging various data in the power industry into the power Internet of Things. After the completion of the terminal construction, this article will start with the big data-based IoT power acquisition and control and power marketing information security, as well as the big data-based power traffic management system security, and elaborate on the big data and the IoT model for the power industry.

3.3. Experimental Platform Development. The power transportation mobile Internet of Things information security platform constructed in this article takes the Hapoop MapReduceV2 framework as the core and establishes a distributed computing cluster through the Map-Reduce programming model to complete the operation and management of the power big data in the system. In the big data storage system, this article uses the manager to manage the system content and serves as an excuse for users to use the client to access data. At the same time, Hadoop is used to complete the construction of distributed clusters, and various data generated by the lines during daily power transmission and distribution are stored in a large number of data nodes to achieve distributed storage. The application layer consists of the Map-Reduce programming model and the distributed

Table 1: Basic protocol format of configuration information data in power transmission node.

Byte	0	1	2-3	4-5	6-10	11-14	15-18	19-20
Description	Data header	Logo	Local address	Target address	Server address	Time stamps	CRC	Data tail
Byte length	1	2	2	2	6	6	4	2

open source database HBase, so that data storage and management can be implemented according to parallel programming and storage excuses.

In the development of terminal collection systems, advanced information technologies such as mobile Internet technology, global positioning system, radio frequency identification technology, mobile communication technology, and intelligent information sensing technology need to be comprehensively utilized. Specifically, it includes a lan communication module for communication maintenance, an identity recognition module for personal information recognition, and a beidou module for precise positioning. In addition, video modules, infrared communication modules, and expansion modules also play important values in the system.

4. Based on Big Data and Internet of Things Technology Research on Electric Traffic Information Security Terminal Architecture

4.1. Big Data-Based Internet of Things Power Acquisition and Control and Power Marketing Information Security Analysis

4.1.1. Security Analysis of Electric Transportation Terminal Based on Big Data. Electricity is an indispensable resource for the normal operation of the country. Therefore, grid operation companies bear heavy responsibilities. They must not only provide high-quality electric energy to all users and ensure the stable operation of users' electrical equipment but also ensure the stability of the entire power grid system and carry out special regulation on power transmission at key nodes. In order to better realize grid management, it is a very correct decision to connect the power industry with big data of the Internet of Things. The transmission system of the power transportation mobile Internet of Things includes three parts: monitoring equipment, application software, and transmission network. In order to ensure the normal operation of the system, its safety must be guaranteed from the system architecture and functions. Table 1 is the basic protocol format of the configuration information data in the power transmission node.

Regardless of the collection node or the transmission node, configuration information is written to the node through the RS485 bus. The configuration information is used to write the local physical address, target physical address, server IP address, time base reference, and other parameters into the node. It can be seen from Table 1 that when a node is identified as a sending node, the target address is the address of the relay node corresponding to the sending; when the node is identified as a relay node, the target address is the address of the standby relay node; when the current relay node is used as a sending node, or the relay forwarding function of the current relay node cannot be used normally, the node forwards information through the standby relay node of the wireless communication module box. In order to further test the transmission delay and correctness of power transmission, this paper evaluates the wireless transmission effect under different distances. Figure 2 is a statistical diagram of the test results of wireless transmission.

It can be seen from Figure 2 that when the transmission distance is within 300 meters, the accuracy of wireless transmission is 100%, and the transmission delay is less than 0.2 milliseconds. But with the expansion of the transmission distance, the transmission delay will continue to increase, and the transmission accuracy rate will continue to decrease. On the whole, the transmission performance of wireless communication within 450 meters is still relatively good. It can be seen that the power transportation mobile Internet of Things information security terminal constructed in this article can realize normal applications in the power field while ensuring the secure transmission of information.

4.1.2. Security Analysis of Internet of Things Power Marketing Information Based on Big Data. The so-called power marketing refers to the power services provided by enterprises in order to meet the power consumption needs of the masses in the power market. The essence of power marketing is to achieve a balance between supply and demand in the power market. With the indepth development of power marketing information, the development of marketing acquisition and control business has become more and more mature in recent years, and the application of automated electrical energy measurement collection devices has become increasingly widespread. The pressure of a large number of automated electric energy metering devices on their uplink databases during operation is also increasing. In addition, there are also certain problems in the storage of acquisition and control systems and power big data. Figure 3 is a statistical diagram of the causes of various equipment failures in the power transportation mobile Internet of Things.

As can be seen from Figure 3, among the causes of various equipment failures in the power transportation mobile Internet of Things, the most frequent occurrence is the integrated access equipment (PCM). In addition, power failures caused by optical cables, cables, and other accessory equipment also have a higher frequency. This paper uses the fuzzy logic toolbox in MATLAB to obtain the support of the fuzzy C-means clustering method to achieve the effect of discretion index. Before clustering the attribute values, first analyze the clustering validity of the number of clustering points.

From the calculation results, the five indicators of optical fiber, PCM equipment, microwave equipment, dispatching switch, and auxiliary equipment occupy a relatively important position in the entire indicator system. Among the index weights, the weight of optical fiber is 0.4697, which is the

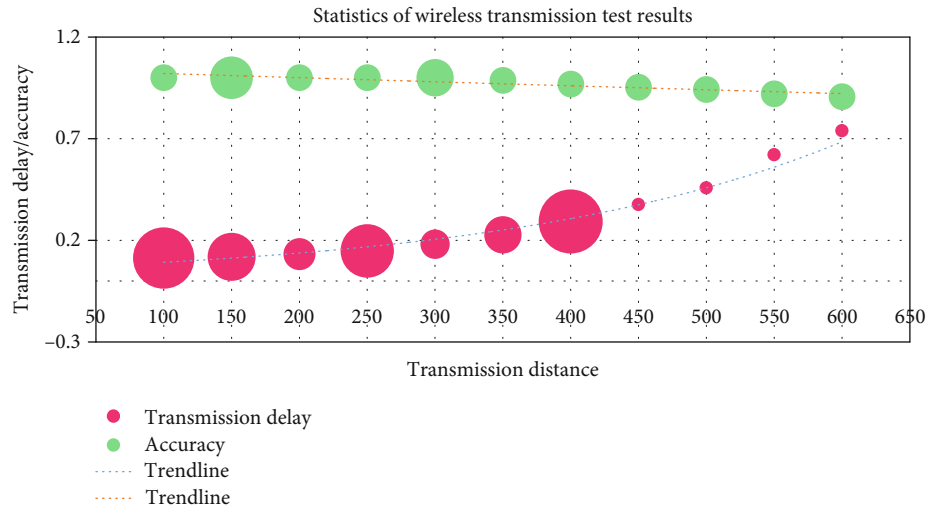

Figure 2: Classification of user resource sharing in agricultural information exchange platform.

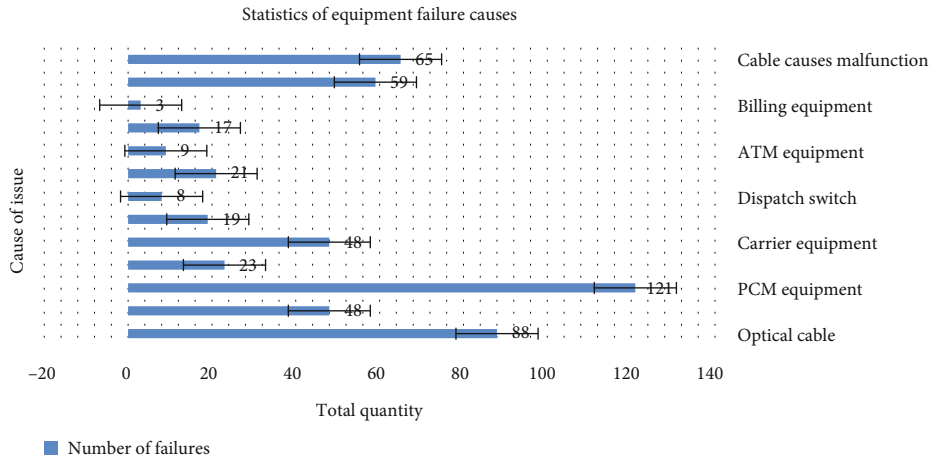

Figure 3: Statistical diagrams of the causes of various equipment failures in the power Internet of Things.

highest among the five indicators. This shows that the safety of optical fiber plays a very important role in the information security of the power, transportation, and mobile Internet of Things.

4.2. Safety Analysis of the Electric Traffic Management System Based on Big Data

4.2.1. Security Analysis of Intelligent Power Monitoring Terminal Based on Big Data. When constructing the information security terminal framework of the electric transportation mobile network, this article adds a monitoring terminal to the terminal collection layer, and the monitoring terminal system includes real-time data collection, data display, data statistical analysis, platform resource management, and predictive warning information. The basic characteristics of the Internet of Things technology include a wide variety of collection terminals, a large number of collected data, a wide range of transmission networks, and intelligent data processing. Therefore, power monitoring terminals developed based on big data and the Internet of Things can better improve the intelligence of the power grid under the premise of ensuring information security. The monitoring system of the mobile power grid is a very important part of the information security framework. The effective visual processing in the monitoring system is precisely because of the auxiliary effect of wireless sensor network technology.

The smart grid is an extremely large system. It is responsible for coordinating the load balance between the user end and the power system. Therefore, it is necessary to monitor the operating status of the equipment in real time to ensure that the equipment maintains normal operation. As the number of users and devices added to the smart grid continues to grow, the amount of data that needs to be monitored in the grid system also multiplies. Therefore, this article starts with improving the control efficiency of smart monitoring terminals and reducing operating costs and improves the monitoring system. Figure 4 is a statistical diagram of power communication consumption.

The improved secret signature scheme in this paper can collect mostly data at the same time and send it to the corresponding recipient. The user can obtain the corresponding

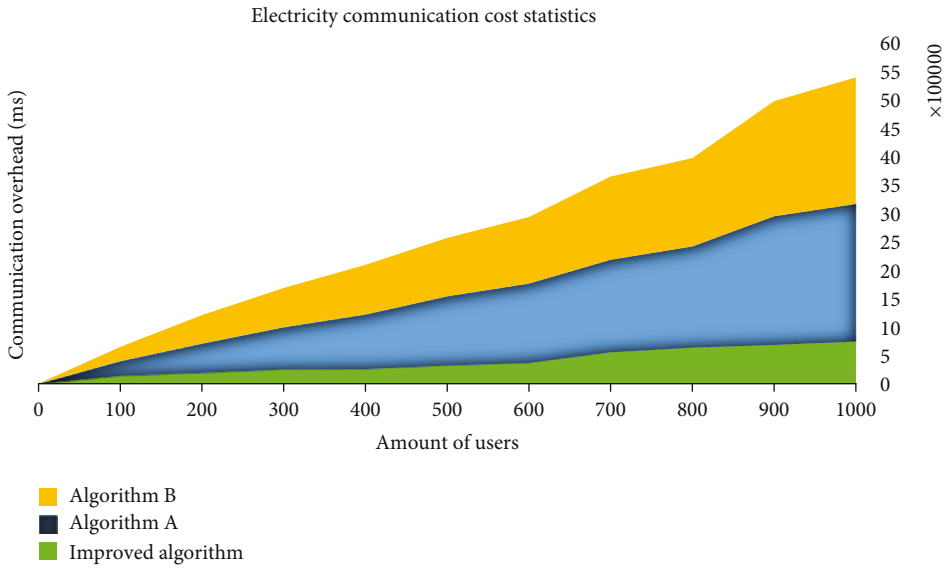

Figure 4: Statistic chart of user power communication overhead with different algorithms.

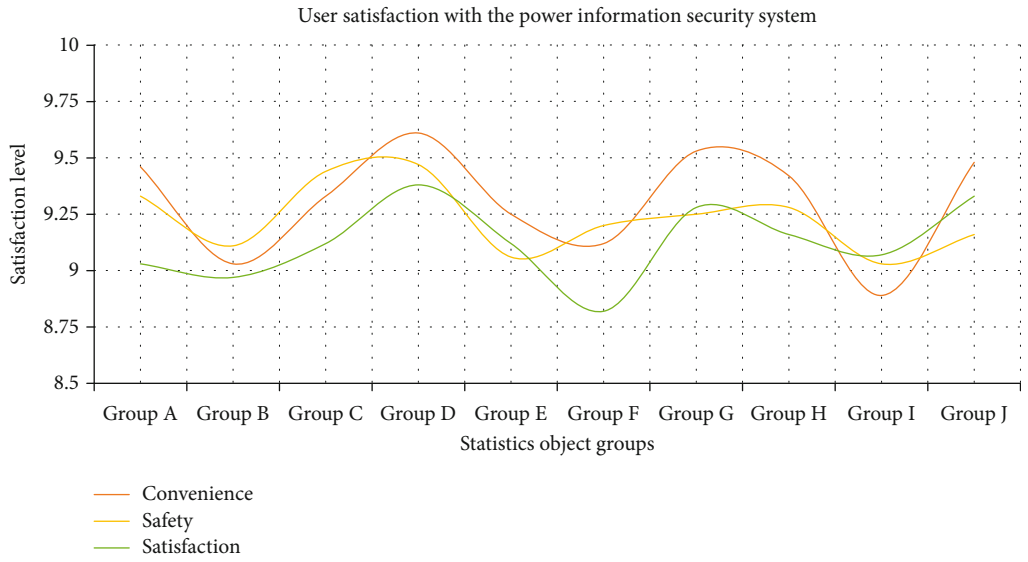

Figure 5: Statistics of user satisfaction with the power information security system.

plaintext information after entering the key. Compared with the two types of traditional algorithm solutions that can only aggregate one-dimensional data, the improved power data monitoring system is obviously more competitive. It can be seen from Figure 4 that comparing the communication resources consumed by the three schemes in the process of aggregating multidimensional data, the improved secret signature scheme significantly saves more communication costs. From a practical application point of view, this solution is used in an intelligent power information security system, which can effectively reduce communication resources and reduce the complexity of system calculations while ensuring information security.

4.2.2. Smart Power Privacy and Security Protection Based on Big Data. When constructing the intelligent power information security terminal based on big data, this article strengthens the data protection function in the information system based on the principle of ensuring data confidentiality, integrity, and nonrepudiation. Even if someone tries to monitor the power communication information, they cannot decrypt it and get the corresponding plaintext. The use of irreversible hashing to achieve data encapsulation can effectively guarantee the confidentiality of data, and the combination of big data and blockchain technology can further ensure the integrity of the data. In addition, since each sensing node has a unique ID as a token when publishing and receiving information, the signed information has nonrepudiation. Figure 5 is the statistical data of users' satisfaction with the intelligent power system. The survey objects are from 10 different communities. The survey method is a questionnaire in the system, and the scoring mechanism is a ten-point system.

It can be seen from Figure 5 that the average scores of users for the convenience, safety. and overall satisfaction of the power system are 9.312, 9.233, and 9.128, respectively. Among the districts B, F, and I with lower scores, the proportion of middle-aged and elderly people living is higher; so, the understanding of the intelligent power security system is also insufficient, while the higher scores in the districts D and G have a significantly higher proportion of young people. In their view, the intelligent power security platform only needs to use the Internet to easily understand the power consumption and complete the electricity bill payment, which improves the convenience of power security services.

5. Conclusions

This paper analyzes the security of power transportation transmission terminal based on big data. This article introduces the power acquisition, control, and transmission terminal based on the Internet of Things technology, analyzes the basic protocol format of the configuration information data in the power transmission node, and tests the core functions of the power transmission system. The experimental results show that the system can indeed meet in engineering practice, and smart grids have high requirements for real-time and reliability of power transmission. This article analyzes the Internet of Things power marketing information security based on big data. The extensive promotion of marketing acquisition and control systems and intelligent acquisition and control terminals has effectively reduced the work pressure of grassroots personnel in the power industry and improved the efficiency of various services in the power system. In order to solve the deficiencies in the traditional information service system, this article analyzes the causes of failures of various devices in the power transportation mobile Internet of Things, improves the problems in the system architecture, and optimizes the existing business service processes.

This article analyzes the safety of the electric traffic management system based on big data. The improved scheme in this paper uses the designed sign cryption algorithm to collect the multidimensional data of the user's power and send it to multiple receivers. In the regulation stage, after the control center analyzes and processes the multidimensional data, it is stored in an immutable and permanent blockchain to achieve efficient management of power data; grid operators can achieve smart contracts for individual consumer power consumption regulation; equipment suppliers can also implement equipment operating status monitoring to ensure that grid equipment operates as usual. This article investigates users' satisfaction with using smart power systems. From the results, most users hold a positive attitude towards the convenience and safety of power information security systems.

This article has carried out research on the construction of power information security terminal based on big data analysis and Internet of Things technology. In order to ensure the safety of power information, it is necessary to take security measures for the entire power information transmission process. Only when the power smart equipment can complete the work smoothly and can the construction and development of the smart grid be further promoted. When looking forward to the future development direction, we believe that the structure and operation mode of the power grid will undergo major changes with the widespread application of new energy and new materials. Therefore, we believe that the focus of future work can be placed on the following aspects: (1) realize more precise control of the smart grid through the Internet of Things technology, (2) combine the big data analysis function to realize real-time grid operation status and carry out fault warning, and (3) realize power of the high degree of integration of industry and information system that provides users with more convenient power services.

Data Availability

The data underlying the results presented in the study are available within the manuscript.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest.

Acknowledgments

This work was supported by the Project of Shandong Province Higher Educational Science and Technology Program (Grant No. J16LN95). This work was supported by the Science and Technology Research Project of Chongqing Education Commission: KJQN202003404.

References

[1] J. K. Kok, M. J. J. Scheepers, and I. G. Kamphuis, "Intelligence in electricity networks for embedding renewables and distributed generation," *Journal of Renewable & Sustainable Energy*, vol. 103, no. 2, pp. 179–209, 2015.

[2] E. Fadel, V. C. Gungor, L. Nassef et al., "A survey on wireless sensor networks for smart grid," *Computer Communications*, vol. 71, pp. 22–33, 2015.

[3] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, "Efficient energy management for the Internet of things in smart cities," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 84–91, 2017.

[4] Y. Jia, Z. Xu, L. Lai, and K. P. Wong, "Risk-based power system security analysis considering cascading outages," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 872–882, 2016.

[5] T. Xiaogang, L. Haiyun, and C. Xiaoxuan, "Control and protection system interface design for multi-terminal HVDC flexible project," *Power System Protection & Control*, vol. 43, no. 9, pp. 124–128, 2015.

[6] S. F. Chang, C. F. Chen, J. H. Wen, J. H. Liu, J. H. Weng, and J. L. Dong, "Application and development of Zigbee technology for smart grid environment," *Journal of Power and Energy Engineering*, vol. 3, no. 4, pp. 356–361, 2015.

[7] S. Hong, S. Park, L. W. Park, M. Jeon, and H. Chang, "An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on

research trends in the security field in South Korea," *Future Generation Computer Systems*, vol. 82, pp. 769–782, 2018.

[8] X. Lu, Z. Qu, Q. Li, and P. Hui, "Privacy information security classification for Internet of Things based on internet data," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, Article ID 932941, 2015.

[9] J. M. Alcaraz Calero and J. Aguado, "MonPaaS: an adaptive monitoring platformas a service for cloud computing infrastructures and services," *IEEE Transactions on Services Computing*, vol. 8, no. 1, pp. 65–78, 2015.

[10] M. B. Alotaibi, "Antecedents of software-as-a-service (SaaS) adoption: a structural equation model," *International Journal of Advanced Computer Research*, vol. 6, no. 25, pp. 114–129, 2016.

[11] S. Costache, D. Dib, N. Parlavantzas, and C. Morin, "Resource management in cloud platform as a service systems: analysis and opportunities," *Journal of Systems and Software*, vol. 132, pp. 98–118, 2017.

[12] Y. Zhu, L. Li, Y. Song, and L. Wang, "Storage and parallel processing of big data of power equipment condition monitoring on ODPS platform," *Diangong Jishu Xuebao/Transactions of China Electrotechnical Society*, vol. 32, no. 9, pp. 199–210, 2017.

[13] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: perspectives and challenges," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 75–87, 2017.

[14] Kaitai Liang, W. Susilo, and J. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1578–1589, 2015.

[15] A. da Veiga and N. Martins, "Information security culture and information protection culture: a validated assessment instrument," *Computer Law & Security Review*, vol. 31, no. 2, pp. 243–256, 2015.

[16] C. Hamon, M. Perninge, and L. Söder, "A computational framework for risk-based power system operations under uncertainty. Part II: case studies," *Electric Power Systems Research*, vol. 119, pp. 66–75, 2015.

[17] J.-S. Cho, Y.-S. Jeong, and S. O. Park, "Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Computers & Mathematics with Applications*, vol. 69, no. 1, pp. 58–65, 2015.

[18] G. Yimin, L. Shundong, D. Jiawei, and Z. Sufang, "Deterministic cloned tag detection protocol for anonymous radio-frequency identification systems," *IET Information Security*, vol. 10, no. 1, pp. 28–32, 2016.

[19] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247–260, 2006.

[20] J. Plata-Chaves, N. Bogdanovic, and K. Berberidis, "Distributed diffusion-based LMS for node-specific adaptive parameter estimation," *IEEE Transactions on Signal Processing*, vol. 63, no. 13, pp. 3448–3460, 2015.

[21] M. Jiang, Y. Li, Y. Ge, K. Lou, and W. Gao, "An advanced DV-hop localization algorithm in wireless sensor network," *International Journal of Control and Automation*, vol. 8, no. 3, pp. 405–422, 2015.

[22] S. Fan and H. Zhao, "Delay-based cross-layer QoS scheme for video streaming in wireless ad hoc networks," *China Communications*, vol. 15, no. 9, pp. 215–234, 2018.

[23] K. M. Abdellatif, R. Chotin-Avot, and H. Mehrez, "AES-GCM and AEGIS: efficient and high speed hardware implementations," *Journal of Signal Processing Systems*, vol. 88, no. 1, pp. 1–12, 2017.

[24] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based approach of generating key-dependent ShiftRows transformation," *International Journal of Network Security & Its Applications*, vol. 7, no. 2, pp. 93–102, 2015.

[25] H. K. Kim and M. H. Sunwoo, "Low power AES using 8-bit and 32-bit datapath optimization for small Internet-of-Things (IoT)," *Journal of Signal Processing Systems*, vol. 91, no. 11-12, pp. 1283–1289, 2019.