Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9931460, 7 pages
https://doi.org/10.1155/2021/9931460

Research Article

Information Security Management of Sharing Economy Based on Blockchain Technology

Jian Xiao

School of Business, Beijing International Studies University, Beijing 100024, China

Correspondence should be addressed to Jian Xiao; xiaojian@bisu.edu.cn

Received 16 October 2021; Revised 22 November 2021; Accepted 2 December 2021; Published 27 December 2021

Academic Editor: Deepak Kumar Jain

Based on the unprecedented development of current information technology, under the prevalence of third-party payment, in order to increase the utilization rate of idle resources and meet the diversified economic needs of today's era, as an emerging economic model-the "sharing economy", combined with Internet big data, it has effectively realized the perfect connection between supply and demand, and it has quickly swept through all walks of life. However, while promoting economic development, the lack of regulatory measures and the imperfect credit system have severely restricted the further development of the sharing economy. Blockchain technology (BT), as a new distributed infrastructure and computing method, has always been the core technology of Bitcoin. Based on the development of generalized economic model and BT, this paper analyzes the shortcomings of generalized economic model and blockchain technology through information fusion big data and proposes a kind of information based on information fusion big data+public BT. The security management system adapts to the status quo of the sharing economy and uses the functions of information fusion big data+blockchain technology to solve the current information security risks faced by the sharing economy. The experimental results of this article show that the sharing economy information security management system based on information fusion big data+blockchain technology has good protection capabilities. The interception rate of external information reached 95%, and the interception rate of system information reached 93%. Better protection of privacy leaks is needed.

1. Introduction

1.1. Background. A new economic model, the "sharing economy," has been gradually developed to allow people to voluntarily contribute to the productive economy based on specific projects and special circumstances. The sharing economy is a new economic growth model based on big data technology. It mainly uses cloud computing databases and Internet network technology to merge and allocate idle resources, thereby avoiding time and space constraints [1]. The sharing economy can make society lose its vitality. The greater value of resources has played an important role in the rational distribution and innovation of social resources. According to my country's economic growth trend, the importance of economic transformation and upgrading to achieve rapid economic growth is self-evident. The distribution of the sharing economy has become an important hub for eliminating social information asymmetry and innovating economic growth models. In the data technology sharing economy model, many problems are gradually exposed, and problems such as information leakage make the integration and development of information fusion big data technology and BT urgent.

1.2. Significance. "Internet+" is a double-edged sword. Although it is easy to manage, it poses a huge security risk to public information security. If these hidden dangers cannot be eliminated in time, they will be brought to the public and the entire country [2]. With the help of Internet information security, the weaknesses of the Internet are endless. Hacking, virus intrusion, enemy surveillance, etc., will damage national defense and directly threaten national security and social stability. In the "Internet +" era, the development of large-scale data and the development of the Internet of Things are all constantly developing [3, 4]. Production and life bring not only convenience but also crisis. Service providers rely on monitored arbitration and may compromise the privacy and security of their users. By promoting the technical integration of big data and BT, the sharing economy can accelerate the process of economic globalization, reduce the operating costs of enterprises, and truly realize the overall progress of the socialist sharing economy in the new era of high information data interaction and high information security.

1.3. Innovation. The innovations of this article are as follows: (1) use information fusion big data to store and process sharing economy information, the BT privacy protection scheme using aggregate signatures, which introduces the core signature algorithm in detail, which is used to verify the legality of the transaction and the identity of the sender of the transaction. (2) The information security system of the sharing economy mainly introduces denial technology and makes full use of the autonomy of agents to improve system functions.(3) Mainly conduct information security protection through information fusion and blockchain technology to prevent hackers from intruding and improve data security.

2. Related Work

Zaharia is working to build a hybrid intelligent system (HIS DIVNAR) based on the synergies of multiple sciences and scientific guidelines for the rapid diagnosis of potential information security intruders. Yankovskaya provides the basis for the proposed method and the construction of DIVNAR for mathematical devices. It consists of four parts. The first part is called ISDIOS and aims at quickly diagnosing human tissue pressure. The third component (DIDEV) is used to quickly diagnose and prevent anomalous behavior. Fourth, it uses cognitive techniques to make and prove decisions using the intelligent and rapid information detection system (IS DINARLOG2) of early popular content-based attacker information security. Various laws include error-tolerant unconditional diagnostics, regularity, and decision-making rules that are resistant to hybrid diagnostic tests [5]. According to a study by Ibrahim, the cloud environment is one of the fastest growing technologies in the IT industry. This is due to reliable and reliable services and the ability to access the "cloud" anytime, anywhere. Providing information security is an important issue for the cloud and ICS. Before implementing ICS in the cloud, it is very important that the ICS organization first determine the information security factors for ICS and the cloud. Failure to identify information security factors can lead to application failures and information loss. For the purposes of this investigation, it uses qualitative methods to investigate the verification of information security factors by professionals [6]. However, there are some differences in the experimental results, as there are not many factors that affect the duration of this experiment. Lee's study argues that economic allocation was an example of a new technology-based tool to improve the efficiency of inert resources utilization. The integration of various parameters and mechanism of allocation of resources became an important tool to increase efficiency and improve service level. BT has no central control system function and can automatically execute smart contracts. BT management has become the most widely used method of economic development as BT has changed significantly to traditional trading methods and financial models. With the advent of the sharing economy model in recent years, there are still many problems in the development of Airbnb and Uber, especially the issue of customer information security, which seriously hinders the development of the sharing economy model. BT functions can solve this problem well, so BT functions facilitate the creation of a common economic model. This article is primarily about information security for customer sharing based on BT. First, we will analyze the relationship between the regional technology of the chain and the sharing economy. Next, we will discuss the security issues facing customer information in the sharing economy. Finally, several information protection strategies and suggestions are provided [7]. However, his experimental process is not over yet.

3. BT Privacy Protection Scheme Based on Aggregated Signature

3.1. The Privacy Protection Needs of BT. Due to the publicity of the BT network, data mining can be used to monitor the transaction process and extract user identity information [8, 9]. For the protection of privacy, it is necessary to address the after two considerations: (1) identity confidentiality refers to keeping the user's true identity and information confidential, even if it is accessed in BT, only limited identity permissions can be provided [10, 11]. (2) Many BT-based applications require confidentiality of transactions, such as electronic medical record management or anonymous identity verification and big data authorization [12, 13]. The classification of common information vulnerabilities is shown in Table 1.

In order to solve this problem, the commonly used method is to shift from a network-centric to a data-centric full lifecycle protection strategy, that is, implement data classification and classification, sort out the data life cycle status, and plan corresponding data encryption, desensitization, auditing and other data protection strategies according to different data sensitivity levels and data usage status to ensure that data security is fully controllable.

3.2. Signature Core Algorithm. For example, in Bitcoin, ECDSAI04, RIPEMDI I0.161, and SHA25107.1081 are used to complete the transaction signature [14, 15]. The detailed description is shown in Figure 1.

As shown in Figure 1, a transaction consists of n inputs and m outputs and has $\sum_{i=1}^{n} \mathrm{in}_i = \sum_{j=1}^{m} \mathrm{out}_j$. By the calculation rule of curves of ellipse, we obtain

$$\sum_{i=1}^{n} \mathrm{in}_i \cdot G = \sum_{i=1}^{n} I_i = \left(\sum_{i=1}^{n} \mathrm{in}_i \right) \cdot G, \qquad (1)$$

Table 1: Information technology vulnerability classification.

Category	Vulnerability (v)	Severity level	Risk level
Behavioral complexity	Sensitivity Predictability	5	High
Adaptation and manipulation	Rigidity Malleability Gullibility	3	Middle
Indirect/nonphysical exposure	Electronic accessibility Transparency	4	High
Direct/physical exposure	Physical accessibility Electromagnetic Susceptibility	3	Middle
Supporting facilities/infrastructures	Dependency	3	Middle

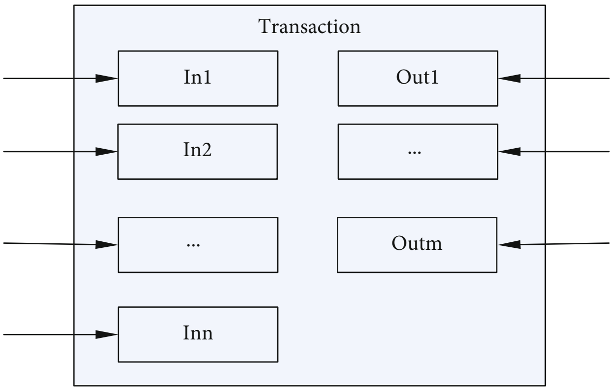

Figure 1: Single transaction model.

$$\sum_{j=1}^{m} \mathrm{Out}_j \cdot G = \sum_{j=1}^{m} O_j = \left(\sum_{j=1}^{m} \mathrm{Out}_j \right) \cdot G, \tag{2}$$

Through equations (1) and (2), we have $\sum_{i=1}^{n} I_i = \sum_{j=1}^{m} O_j$, we can verify $\sum_{i=1}^{n} \mathrm{in}_i = \sum_{j=1}^{m} \mathrm{out}_j$, because the attacker cannot get in_i and out_j through I_i and O_j.Through the cone circle algorithm, we can get

$$\begin{gathered} \sum_{i=1}^{n} \mathrm{in}_i \cdot G = \left(\sum_{i=1}^{n} \mathrm{in}_i \right) \cdot G, \\ \left(\sum_{i=1}^{n} \mathrm{in}_i \right) \cdot G = \sum_{i=1}^{n} \mathrm{in}_i \cdot G. \end{gathered} \tag{3}$$

Further, you can get

$$\left(\sum_{i=1}^{n} \mathrm{in}_i \right) \cdot G = \sum_{i=1}^{n} (\mathrm{in}_i \cdot G). \tag{4}$$

In the normal network, the sum of all input amounts is

$$\mathrm{Is} = \sum_{i=1}^{n} \mathrm{in}_i - \sum_{j=1}^{u} \mathrm{int}_j. \tag{5}$$

The sum of all output amounts is

$$\mathrm{Os} = \sum_{i=1}^{n} \mathrm{out}_i - \sum_{j=1}^{u} \mathrm{out}_j \tag{6}$$

The set $\{\mathrm{int}_j\}_{1 \le j \le u}$ and $\{\mathrm{out}_j\}_{1 \le j \le v}$ are the set $\{\mathrm{int}_i\}_{1 \le i \le u}$, a subset of $\{\mathrm{out}_i\}_{1 \le i \le u}$. Because it is easy to get $\sum_{i=1}^{u} \mathrm{in}_i = \sum_{j=1}^{v} \mathrm{out}_j$ and $\sum_{i=1}^{n} \mathrm{in}_i = \sum_{j=1}^{m} \mathrm{out}_j$. Through the application of the above formula, the data information of this transaction can be obtained, and the data security can be guaranteed to a certain extent.

3.3. Protection Methods of BT Transaction Privacy. BT has its own agreement and can only access the computer through the agreement. Only when the user uses the designated computer can the corresponding data information be read.

There are two main methods to protect the confidentiality of BT transactions, namely, noninteractive zero-knowledge proof (NIZK) and homomorphic cryptography [11, 16].

(1) Zero-knowledge noninteractive proof, including the prover and verifier [17]: for a sentence, the prover can create a proof to persuade the verifier to recognize the correctness of the sentence [18]. In this process, the verifier can only know that the Dao proposition is correct (possibly zero knowledge). Zero-knowledge evidence is divided into interactive and noninteractive. The zero-knowledge interactive proof requires several rounds of exchanges between proverbs and the verifier to complete the zero-knowledge noninteractive proof (NIZK) does not require an interactive process between the verifier and the verifier and is more suitable for difficult scenarios for and verification. The program is connected at the same time [19]

(2) Homomorphic cryptographic system: homomorphic cryptography (HC) is an encryption method that satisfies homomorphism. The arithmetic operations performed in the form of cipher text can be maintained [20]. Allows calculate encrypted currency

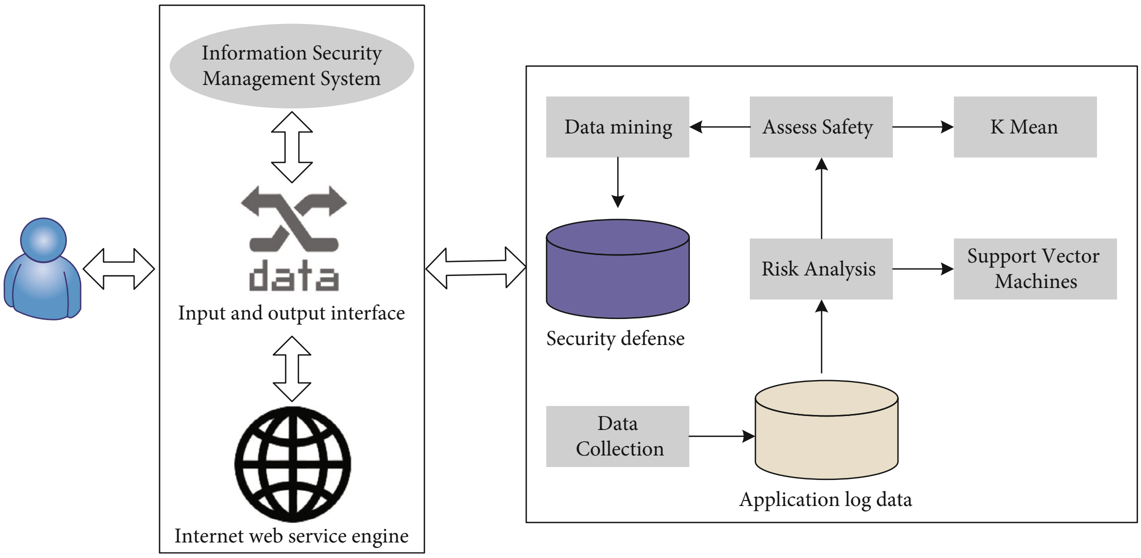

Figure 2: Flow chart of information security management of sharing economy based on information fusion big data.

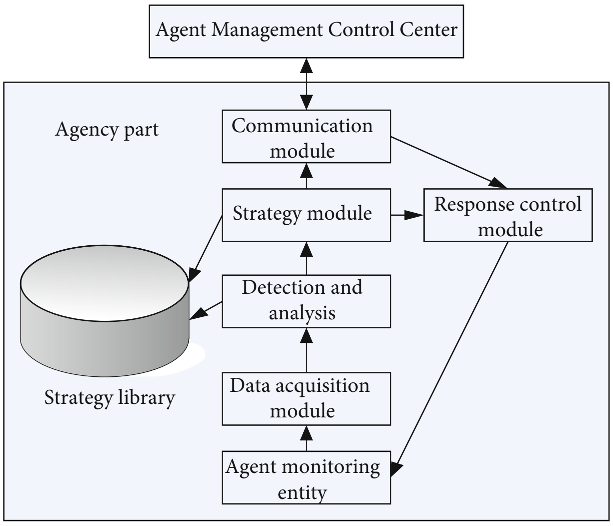

Figure 3: Detailed design of the agent.

anywhere, while protecting the privacy of digital data. Operates as a black box□when n encryption sum functions are given, the encryption result of the same function will be exported to the corresponding original data. This attractive feature makes homomorphic encryption very suitable for hiding and updating transaction amounts and other metadata [21]

Zero-knowledge proof is a method by which one party can prove to the other party that they know the value x without conveying any information, except that they know the value x. The essence of zero-knowledge proof is that it is trivial to prove that someone has knowledge of certain information by simply revealing the information. Fully homomorphic encryption is regarded as the holy grail of information security because it can protect the privacy of data stored in the cloud or in transit.

4. Design of Information Security Management System

The information security management system involves a lot of information, and it is necessary to analyze the correlation of information to achieve the simplification of the information [11]. In addition, the system can also customize the data collection policy rules as needed to BT the desired information. The network security management system needs to realize the interaction of network security equipment through linkage modules to achieve the overall protection effect of the network. These functions require related modules based on agent technology to achieve [22]. Below, we discuss in detail the related design and implementation of the proxy module.

4.1. Application Design of Information Fusion Big Data in Information Security Management System. Information fusion big data technology was used to process information data, concentrate information, conduct risk analysis and security assessment of information, and realize information security management. The information security management process of the sharing economy based on information fusion big data is shown in Figure 2.

4.2. Agency Design. The agent is the basic detection unit of the system, which is used various safety equipment. A variety of agents can be configured on the security device to collect various required information according to needs. In the system, each agent has its own independent information source and detection mode and can independently realize the detection task. At the same time, each agent can cooperate with each other or work together under the control of the agent control center, refer to Figure 3 for detailed agent design;

4.3. Design of Agent Management Control Center. The agent management control center mainly completes the remote

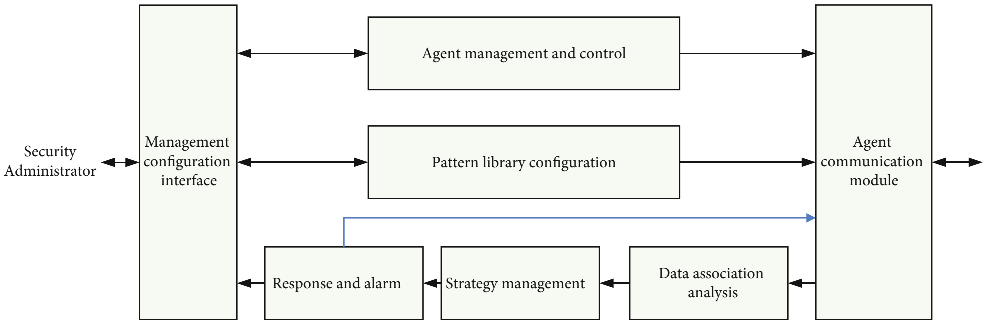
Security Administrator
Management configuration interface
Agent management and control
Pattern library configuration
Agent communication module
Response and alarm
Strategy management
Data association analysis

Figure 4: Structure diagram of the agent management control center.

Table 2: Confirmatory analysis results.

Dimension	Question type	Model parameter estimates				Reliability and validity		
		Non-standardized	S.E	C.R	Standardized	SMC	CR	AVE
Network controller	Q1	1.025	0.125	8.152	0.856	0.452	0.796	0.562
	Q2	1.083	0.122	8.253	0.255	0.523		
Surroundings	Q3	0.856	0.128	9.235	0.552	0.853	0.965	0.532
	Q4	1.235	0.862	23.25	0.568	0.529		
Technology	Q5	1.123	0.238	8.623	0.961	0.533	0.862	0.522
	Q6	0.632	0.258	4.253	0.523	0.423		
Information security	Q7	0.992	0.128	4.523	0.742	0.532	0.965	0.823
	Q8	0.890	0.035	9.128	0.853	0.426		
Standard		—	>0	>1.85	<0.05	>0.5	>0.7	

Table 3: Adaptation index.

Simulation fitting coefficient	Statistics	Optimal standard value	Fit
Bangla	101.562	—	—
Degree of freedom	48	—	—
Chi-square/degree of freedom	2.121	<3	Great
RMSEA	0.078	<0.05	Great
GFA	0.853	<0.8	Great
AGFI	0.852	<0.9	Accept

configuration and management of the agent, the management of the pattern library, the data association analysis from the agent, and the alarm and response functions. The agent management control center can prevent data leakage and loss through centralized management of data and ensure data security to the greatest extent. At the same time, the agent management control center system can conduct comprehensive scheduling management of data information to prevent data from being illegally analyzed and stolen. Once there is an abnormal situation of data information, the system will automatically alarm. The main modules of the agent control center are as follows: agent management and configuration module, pattern library management module, data association analysis module, linkage module, response and alarm module, and management configuration interface, refer to Figure 4 for the detailed design of the agent management control center.

4.4. Agent System Implementation. Data sources for data collection include host data sources and network data sources [23, 24]. Among them, the network data source collection part mainly records, filters, and formats the network connection information of the monitored host system, and then writes it into the log file; the data source on the host mainly includes the storage of system logs and various audit records. It mainly realizes the collection and processing of network data sources.

5. Experimental Analysis of Information Security Management System

5.1. System Reliability Analysis. For the accuracy and validity on the survey data of the questionnaire, we verified as well as analyzed and processed the experiment. Process exclusion of those data with load < 0.6, with the results of validation demonstrated in Table 2.

The standard error (SE) of all model observation variables below the estimated value of the non-standard model in Table 2 is greater than zero. This table shows that the results of the confirmatory analysis meet the reliability and validity requirements. This proves that the quality of the survey data is very good, and we can take the next step in processing the data.

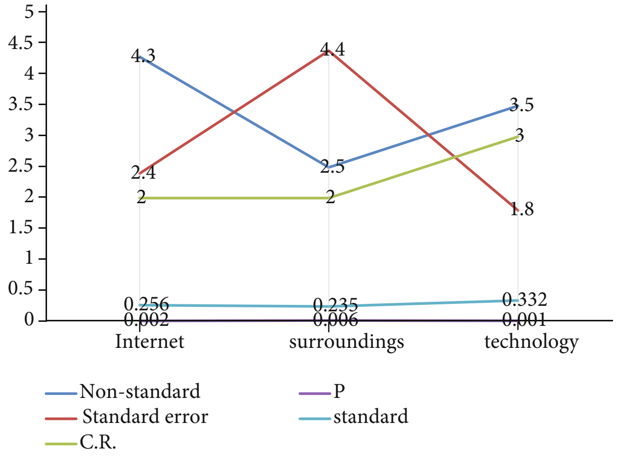

FIGURE 5: Model assumptions and parameter estimation.

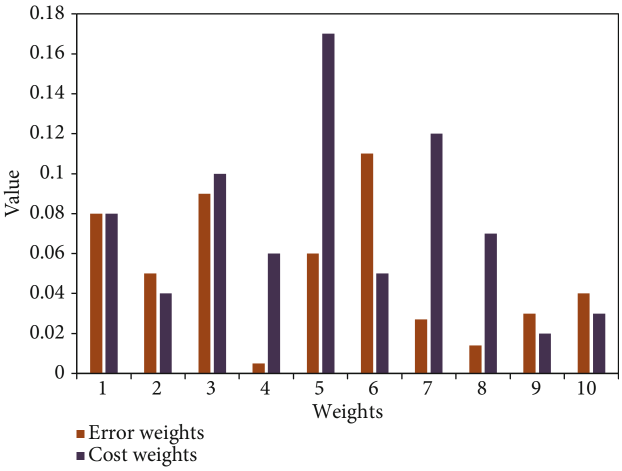

FIGURE 6: Error weight and technology cost weight.

5.2. Research Hypothesis Test Analysis. The structural equation model fits well which shows that the model is constructively reasonable and has credible results, as can be seen from Table 3. Convincing estimates of the structural equations for the study system with associated components are shown in folded Figure 5.

It is evident from Figure 5 in that the relevant parameters in the research hypothesis meet the criterion of significance. It is meaningful to construct a network information security assessment system from the perspective of personal network control, environment and technology, and the impact factor can be used as a security indicator.

As shown in Figure 6, the weight of each vulnerability and security technology is randomly assigned. In order to ensure the comparability of the experimental results, a weight map of vulnerabilities and security technologies was selected by experts.

From Figure 7, it can be found that the error rate of the information management system vulnerability is less than 2%. It is found that the larger the number of particle swarms, the lower the error. The speed of operation increases exponentially as the scale of the problem increases. It can minimize the investment cost of security technology and maximize the effect of vulnerability processing.

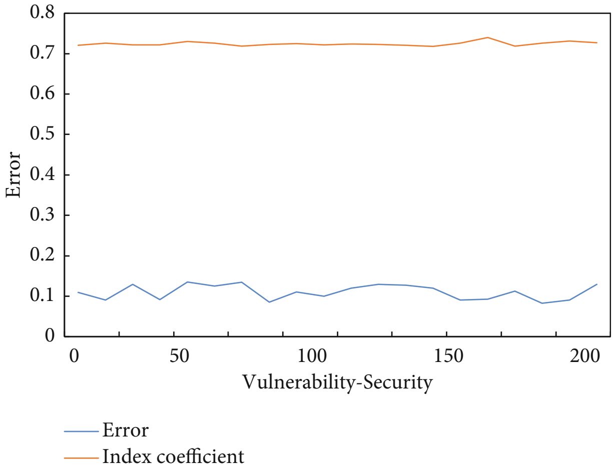

FIGURE 7: Sharing economy information security management system error.

6. Conclusions

We analyze the application in the sharing economy information securing of information fusion big data and BT in this paper. It was found through the analysis that BT showed many similarities on the model of economy of share. BT and sharing economy are essentially P2P platforms, and public BT can physically adapt to the sharing economy model. The characteristics of decentralized and stored non-information leakage and information traceability provide an effective solution to the information security problem in the development of the exchange economy. At the same time, the agent technology is introduced to design the information security management system, and the autonomous function of the agent is fully utilized to improve the performance of the network security management system, making the system more powerful in information processing functions. The security management system that has better scalability and stability and surpasses the traditional security management system has a shortcoming, that is, insufficient information processing and response.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this article.

References

[1] S. Namasudra and P. Roy, “PpBAC,” *Journal of Organizational and End User Computing*, vol. 30, no. 4, pp. 14–31, 2018.

[2] Z. Lv, A. K. Singh, and J. Li, “Deep learning for security problems in 5G heterogeneous networks,” *IEEE Network*, vol. 35, no. 2, pp. 67–73, 2021.

[3] X. Li, H. Liu, W. Wang, Y. Zheng, H. Lv, and Z. Lv, "Big data analysis of the internet of things in the digital twins of smart city based on deep learning," *Future Generation Computer Systems*, vol. 128, pp. 167–177, 2021.

[4] Z. Lv, R. Lou, J. Li, A. K. Singh, and H. Song, "Big data analytics for 6G-enabled massive internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5350–5359, 2021.

[5] M. Zaharia, R. S. Xin, P. Wendell et al., "Apache Spark: a unified engine for big data processing," *Communications of the ACM*, vol. 59, no. 11, pp. 56–65, 2016.

[6] A. Ibrahim and J. H. Yahaya, "Information security factors in the implementation of industrial control system into cloud environment," *Advanced Science Letters*, vol. 24, no. 7, pp. 5239–5242, 2018.

[7] J. A. Lee, "Tripartite perspective on the copyright-sharing economy in China," *Computer Law & Security Review*, vol. 35, no. 4, pp. 434–452, 2019.

[8] S. V. Bharathi, "Prioritizing and ranking the big data information security risk spectrum," *Global Journal of Flexible Systems Management*, vol. 18, no. 3, pp. 183–201, 2017.

[9] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: privacy and data mining," *IEEE Access*, vol. 2, no. 2, pp. 1149–1176, 2017.

[10] Z. Obermeyer and E. J. Emanuel, "Predicting the future-big data, machine learning, and clinical medicine," *The New England Journal of Medicine*, vol. 375, no. 13, pp. 1216–1219, 2016.

[11] S. Athey, "Beyond prediction: using big data for policy problems," *Science*, vol. 355, no. 6324, pp. 483–485, 2017.

[12] Q. Da, J. Sun, L. Zhang et al., "A novel hybrid information security scheme for 2D vector map," *Mobile Networks and Applications*, vol. 23, no. 4, pp. 734–742, 2018.

[13] D. Zou and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," *IEEE Photonics Journal*, vol. 8, no. 5, pp. 1–9, 2016.

[14] B. Edelman, M. Luca, and D. Svirsky, "Racial discrimination in the sharing economy: evidence from a field experiment," *Applied Economics*, vol. 9, no. 2, pp. 1–22, 2017.

[15] C. Narasimhan, P. Papatla, B. Jiang et al., "Sharing economy: review of current research and future directions," *Customer Needs and Solutions*, vol. 5, no. 1-2, pp. 93–106, 2018.

[16] M. Chen, Y. Ma, J. Song, C. F. Lai, and B. Hu, "Smart clothing: connecting human with clouds and big data for sustainable health monitoring," *Mobile Networks & Applications*, vol. 21, no. 5, pp. 825–845, 2016.

[17] I. Hashem, V. Chang, N. B. Anuar et al., "The role of big data in smart city," *International Journal of Information Management*, vol. 36, no. 5, pp. 748–758, 2016.

[18] K. Zhou, C. Fu, and S. Yang, "Big data driven smart energy management: from big data to big insights," *Renewable & Sustainable Energy Reviews*, vol. 56, pp. 215–225, 2016.

[19] S. Akter and S. F. Wamba, "Big data analytics in E-commerce: a systematic review and agenda for future research," *Electronic Markets*, vol. 26, no. 2, pp. 173–194, 2016.

[20] Y. Zhang, M. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2017.

[21] N. Vithanwattana, G. Mapp, and C. George, "Developing a comprehensive information security framework for mHealth: a detailed analysis," *Journal of Reliable Intelligent Environments*, vol. 3, no. 1, pp. 21–39, 2017.

[22] A. D. Mauro, M. Greco, and M. Grimaldi, "A formal definition of big data based on its essential features," *Library Review*, vol. 65, no. 3, pp. 122–135, 2016.

[23] G. Chen, Y. Lu, Y. Meng et al., "Fuso: fast multi-path loss recovery for data center networks," *IEEE/ACM Transactions on Networking*, vol. 26, no. 3, pp. 1376–1389, 2018.

[24] Z. Lv and H. Song, "Trust mechanism of feedback trust weight in multimedia network," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 4, pp. 1–26, 2021.