Research Article

Model Design of Big Data Information Security Management Based on the Internet of Things

Jian Yao

Security Office, Lianyungang Technical College, Lianyungang 222000, Jiangsu, China

Correspondence should be addressed to Jian Yao; 1995120061@lygtc.edu.cn

Received 27 July 2022; Revised 20 September 2022; Accepted 27 September 2022; Published 10 October 2022

Academic Editor: Tarni Mandal

At present, the level of modernization and informatization is constantly improving, especially in rapidly developing China. A large amount of information is collected every second, forming a huge database and making people live in the "big data era." Following cloud computing and the Internet of things, big data technology has become another revolutionary change in the global society, changing global development and becoming a new development point for technological innovation, industrial policy, and national information security. Big data in the new age poses new challenges and perspectives for the nation’s infosec development. Big data is a renewed tool for state security. Nations use big data to create state infosec, offering great facilitation, potential for adoption, and business value. This is a "new blue ocean" for competition among countries. Although big data brings convenience to public life, it also poses a serious threat to national information security. After the research and experiment of the model design of big data information security management of the Internet of things, the experimental data have shown that 86.67% set passwords in communication devices and storage devices. 66.67% installed firewalls, and 76.67% ran antivirus software. Compared with before, the total ratio of setting a password increased by 53.34% and the total ratio of installing a firewall and running antivirus software both increased by 26.67%. It can be seen from the above data that the protection of big data information under the Internet of things has been significantly improved. From the above data, through the big data information security management of the Internet of things, a new development direction is proposed for the development of information security.

1. Introduction

With the continuous innovation and breakthrough of science and technology, and the continuous development of network technology and information industry technology, data resources have become an important social resource and industrial resource, which has been paid more and more attention and attention by people. From the development of the era of big data to today, the concept and application of big data technology has long been beyond the scope of academia. It has also entered into all areas of social life and can be said to be all-encompassing and omnipotent. National information security is the foundation of a country and the foundation for defending the country and maintaining the stability and prosperity of the nation. It is a question of the existence and evolution of the state, and it is also an important guarantee for the people of the country to live and work in peace and contentment. Only when the country is safe, the economy can develop, the nation become prosperous, society is harmonious, the "Chinese Dream" can be realized, and a new chapter in China can be written. With information development and the advent of the big data era, the speed of information development and dissemination far exceeds people’s imagination. The challenge to information security is unprecedented, so people must seriously study and explore how to ensure information security while facing challenges and opportunities and put forward reasonable and appropriate countermeasures and suggestions.

Now that people have entered the era of Internet+, big data has developed rapidly. A mobile phone, a QR code, and a virtual account can buy and sell goods, pay money, and socialize, while big data brings us convenience and speed,
and it also provides opportunities for lawbreakers and hostile forces. Through this new way of using big data, they can take advantage of the impact on national information security to steal state secrets, economic and commercial secrets, protect privacy, and engage in other illegal and criminal activities. At present, China has risen to become the country with the largest number of Internet users and the largest number of smartphone users in the world. However, because China’s information security assurance is in its initial stage, there are not many laws and regulations related to information security, especially national information security. There is no national and social supervision mechanism, and the application level of science and technology is relatively backward. There are not many core technologies with patents, resulting in the flood of network data and rampant underground illegal “data industry chain” activities. Therefore, it is very important to conduct in-depth research on big data information security management from the perspective of the Internet of things to discuss challenges and impacts brought by the Internet of things and big data and explore response policy.

After research on the model design of the big data information security management of the Internet of things, the data showed that based on the loss of big data information based on the Internet of things, 60 people were attacked on the contact equipment, accounting for 20%. Communication equipment was lost in 9 people, accounting for 3%; storage equipment was lost in 15 people, accounting for 5%. Compared with before, the number of people who were attacked by contact equipment decreased by 140 with a total decrease of 46.67%; the number of people whose communication equipment was lost decreased by 41 with a total decrease of 13.67%; the number of people who lost storage devices decreased by 85 with a total decrease of 28.33%. From the above data, it can be seen that after the research and experiment of big data information security management of the Internet of things, it is of great relevance in facilitating the present evolution of infosec.

2. Related Work

This paper studied some technologies of big data information security management, which can be applied sufficiently in the area. Lin studied the scheduling problem of hybrid critical systems with fault tolerance [1]. Liu and Hu elaborated the definitions of proactive technology, and some examples of active violence are given [2]. Nitsche reviewed community security sources for working cooperatively and reviewed the persistent issues of continuing challenges and obstacles to sharing security messages effectively [3]. The research study conducted by Wang et al. believed that the information value chain can help reveal the impact of IT-induced drug administration mistakes on healthcare delivery processes and individual patients [4]. Mcwen et al. improved the opportunities for environmental health and safety staff and chemical informatics specialists to provide support services for conducting laboratory risk assessments [5]. Those approaches inform the study of this text somehow, but they are not publicly acceptable owing to the brevity of the associated period of research and the smaller sample size.

Based on the Internet of things, the following relevant materials were reviewed to optimize the research on big data information security management. Perera et al. surveyed over 100 IoT smart concepts in the markets and examined each of them to ascertain the skills, capabilities, and applications of them [6]. Collier believed that the Internet is the product of revolutionary advances in electronics, telecommunications and information technology, equipment, and applications [7]. Smruti and Sarangi proposed a new taxonomy of IoT technologies. They introduced some important technologies and outlined some applications that may have a significant impact on human life [8]. Mosenia and Jha briefly described three well-known IoT reference models and defined security in the context of IoT [9]. Security and private matters in the IoT landscape were addressed by Alrawais et al. They presented a scheme to use fog to enhance security by utilising it to improve the allocation of credential rejection info between IoT appliances [10]. Zarpelao et al. reviewed the research work of IoT intrusion detection systems [11]. These methods provide a sufficient literature basis for research on the big data information security management of the Internet of things.

3. Overview of IoT and Big Data Information Security

In the current era of big data, information security is facing major challenges, and an invisible large-scale war is in full swing. Therefore, this paper pushed the development of big data security management to a new height through the research on the Internet of things.

3.1. Overview of IoT. As an extension of the current Internet, the Internet of things provides communication capabilities for physical entities in the real world through sensing technology to interconnect, communicate, and interact between different entities. It enables things to connect and talk to each other, just as people communicate with each other through the network on the Internet, and “activates” objects. By giving full play to capabilities of different types of physical entities, they can jointly meet the application needs of different fields, realize extensive interconnection, and truly achieve “Internet of Everything.” As the study of IoT continues to grow, more and more application fields have realized Internet of things solutions in the field according to their own application requirements, including public facilities, automobile transportation, smart city urban agriculture, and medical care. [12]. Most of the IoT applications involved are dedicated to reducing production costs, optimizing processing processes, realizing the safety and convenience of production and life, and providing comfortable living assistance.

The basic concept of the Internet of things (IOT) emerged in the late 1990s and caught the attention of governments, researchers, and various industries. The Internet of things is a huge information network that connects everything in the
world. However, IoT is mainly concerned with the management of things and the connection of things, not the connection between sensing devices and things, that is, the connection between objects and surrounding objects and even the social relationships among various smart objects throughout the Internet of Things. A social relationship is a general term for various complex relationships between people in a social network (SN). Then, in IoT, technical connections are relationships among physical objects. Through the owner relationship of objects, the human-human interaction process is introduced into the Internet of things, which will form a comprehensive perception system with social attributes and realize the social Internet of Things (SIoT) that has a comprehensive perception of human society.

The social Internet of things is a new application of Internet of things technology in social networks, which is still in a state of development. In the past couple of years, the concept of making social connections to things in the Internet of things with social web-based elements has become widespread. The social Internet of things can be seen as a combination of traditional peer-to-peer networks and social networks and is a new application of Internet of things technology in social networks. Unlike traditional service-oriented peer-to-peer networks, local social systems and social connections play an essential part in the social Internet of things, where objects (real or virtual) are basically manipulated or worked for by humans. Therefore, the social relationship between users/providers must be considered during the design phase of social IoT applications. A system of social IoT can be thought of as a peer-to-peer (P2P) web of communities centred on the owner, with devices (owned by people) asking and delivering on behalf of service providers [13, 14].

The Internet of things is a worldwide network of standard telecommunication protocol-based connected entities, consolidating a large variety of disparate and omnipresent entities that generate constant messages about the actual physical world. By placing smarts into daily items, they are converted into clever items that not just collect intelligence from their surroundings but also connect or control the actual physical world to inform each other in order to allow the interchange of data and messages via the web. The Internet of things information function model is shown in Figure 1.

The Internet of things is an essential element of the new wave of technology, and the Internet is its core and basis, where each object can exchange and transmit information and form a “social network” composed of objects. The functional model of the Internet of things is to directly connect item information to the Internet and social networks, pushing the limits of social network time, space, and participating objects, realizing a new system of deep integration of the virtual world and the real world, and establishing an Internet of everything that enables the physical world to coexist with human society [15].

In a service-based IoT system, the functionality provided by each entity can be considered as a service. According to different classification standards and scopes, IoT offers can be classified into three categories based on their capabilities: message-related based services, operational services, and logical services. All of these have atomic services, and the composite service consists of a full set of IoT system services. Information-based services perform information collection, storage, and retrieval, detect changes in objects in the external environment, and transmit the received information to other services. Operation-based services can communicate with controlled objects in the environment [16]. Logical services analyze, calculate, and provide input tailored to the customer’s needs and then realize the purpose of generating commands according to the predefined business logic. The IoT service model is shown in Figure 2.

In terms of IoT services, it is not only necessary to meet the functional goals of users but also to improve user satisfaction as much as possible. From the perspective of users’ use, QoS of services mainly includes correctness, security, accessibility, reliability, availability, integrity, standardization, and robustness. Considering the satisfaction of users, service QoS includes credibility, reliability, service price, execution time, response time, security, and throughput.
Therefore, although there are many QoS attributes of services, according to user needs, service requests can be classified as functional or nonfunctional [17].

Based on the Internet of things to achieve the goal of interconnecting everything at any time and anywhere, in order to effectively manage the resources existing in the Internet of things, it is first necessary to research and analyze the architecture of the Internet of things. Then, according to the measurement indicators of different IoT architectures, a reasonable resource management method is effectively established.

In the IoT-based REST network service architecture, the implementation difficulty of services is reduced through standardized operation methods. Combined with other Internet standard technologies such as URI, HTML, and XML, it can effectively improve the communication interaction between physical devices. Currently, REST-based web services are the most widely used method to realize the interaction of physical devices to build IoT systems. Among them, IoT-A is a REST-like architecture for horizontal connection of local IoT systems. The IoT-A architecture reference model is shown in Figure 3.

IoT-A provides services by abstracting local IoT systems with different sensors and communication systems into a unified IoT resource model that is divided into several layers based on device roles, functional granularity, and abstraction levels. It includes various layers such as device connection and service layer, resource layer, virtual entity layer, process execution and service combination layer, and application layer. By designing application requirements in the form of business processes, IoT systems can become more flexible and widely applicable [18].

The Internet of things (IoT) is a network that connects sensor-equipped objects to the Internet through protocols, using devices such as global positioning systems, radio frequency identification (RFID) devices, infrared sensors, and laser scanners to collect data for intelligent identification, tracking, positioning, controlling, and monitoring of data exchange and transmission. The entire network is divided into three layers: First, the identification network, that is, the use of sensors, RFID devices, QR codes and so on to identify “things.” The second is the transmission network, that is, the use of the existing three kinds of networks (Internet, broadband network, and telecommunications network) or the next generation network (NGN) for computing and data transmission. Third, the application network, that is, the input and output control points, such as mobile phones and smart device controllers. This Internet-based but distinctly different IoT network structure from the traditional Internet offers the following possibilities. The first is large-scale sensing, that is, the use of RFID, sensors, etc., to obtain object information anytime, anywhere. The second is reliable transmission, that is, through the integration of various telecommunication networks and the Internet, the target information can be transmitted accurately in real time. The third is intelligent processing, that is, analyze and manipulate large volumes of data and messages using various intelligent computing skills, such as cloud gaming, and regard intelligent processing and overall perception as the key content of the Internet of things. The network structure adopted by the Internet of things and its characteristics.
determine that the information security problems faced by the Internet of Things not only include the problems presented by the current Internet but also face more new problems that are complex, more severe, and more difficult to deal with, which directly challenge the healthy and sustainable development of the IoT industry [19–21].

The physical layer key generation method uses the wireless channel used by both legitimate communication parties to extract the key. In recent years, it has attracted extensive attention in both academia and industry. Some scholars have proved that physical layer key generation can achieve perfect encryption from an information theory point of view, which provides a new idea for the distribution and management of keys in wireless communication systems.

The key generation technology of the wireless physical layer allows legitimate communication parties to extract the key using the shared information on the wireless channel, without the need for key distribution, and the implementation complexity is low, so it is more suitable for the Internet of things. In the channel detection stage, the training sequence $m_B$ is obtained by using the zero-forcing algorithm:

$$
\bar{h}_{BA} = \frac{m_B^T}{\|m_B\|^2} y_B.
$$

(1)

The training series $m_A$ is obtained by using the zero-forcing algorithm:

$$
\bar{h}_{AB} = h_0 + \frac{m_A^T}{\|m_A\|^2} y_A.
$$

(2)

The abovementioned formulas realize the sharing of private information through the method of channel detection, and then, the two can use this as the key source to generate a consistent key $K$ by performing key negotiation on the public channel, which must satisfy

$$
\frac{1}{y} I (K; \varphi) \leq \varepsilon,
$$

$$
\frac{1}{y} H (K) \geq R_S - \varepsilon,
$$

$$
\frac{1}{y} \log |L| \leq \frac{1}{y} H (K) + \varepsilon.
$$

(3)

Among them, $L$ is the limited character set of key $K$ [22]. According to the key generation model, the key capacity of the generated key can be obtained as follows:

$$
C_S = \max I (n_A; n_B).
$$

(4)

Combining the abovementioned formula, the Markov relation can be obtained as follows:
\[ \tilde{h}_{AB} \rightarrow n_A \rightarrow h_0 \rightarrow n_B \rightarrow \tilde{h}_{AB}. \]  

According to the Markov relation, it is easy to get

\[ I(\tilde{h}_{BA}; \tilde{h}_{AB}) \leq I(n_A; n_B). \]  

By analyzing the abovementioned formula, the new Markov relation can be obtained as follows:

\[ n_A \rightarrow \tilde{h}_{BA} \rightarrow h_0 \rightarrow \tilde{h}_{AB} \rightarrow n_B. \]  

Similarly, it can be concluded that

\[ I(n_A; n_B) \leq I(\tilde{h}_{BA}; \tilde{h}_{AB}). \]  

In this way, the abovementioned formula can be combined to get

\[ I(\tilde{h}_{BA}; \tilde{h}_{AB}) = I(n_A; n_B). \]  

The proof formula is established. According to the formula, the key rate is as follows:

\[ R_S = \frac{1}{T} I(\tilde{h}_{BA}; \tilde{h}_{AB}). \]  

Among them, \( 1/T \) is the normalization factor. The channel gain is fixed within \( T \) symbol periods. Therefore, only one set of random variables can be observed in every \( T \) symbol period [23].

Since both \( \tilde{h}_{BA} \) and \( \tilde{h}_{AB} \) are noisy estimates of the channel \( h_0 \), they are not completely consistent due to the existence of noise. Directly quantizing and generating the key will generate some inconsistent bits, which need to be reconciled through the key negotiation stage. At the same time, during information reconciliation, the information of the key source should not be leaked or leaked as little as possible so as to achieve the reachable key rate \( R_S \).

The joint source \((M, N)\) distributed source coding consists of two coding maps, as shown in the following formulas:

\[ f_1: m^y \longrightarrow \{1, 2, \ldots, 2^{R_1}\}; \]
\[ f_2: n^y \longrightarrow \{1, 2, \ldots, 2^{R_2}\}. \]  

It also contains a decoding map, which can be expressed as follows:

\[ g: \{1, 2, \ldots, 2^{R_1}\} \times \{1, 2, \ldots, 2^{R_2}\} \rightarrow m^y \times n^y. \]

Among them, \( f_1(m^y) \) corresponds to the subscript of \( m^y \), \( f_2(n^y) \) corresponds to the subscript of \( n^y \), and \((R_1, R_2)\) is the encoded bit rate pair [24].

3.2. Overview of Big Data Information Security. In the era of big data, with the rapid progress of information data collection efficiency and the gradual improvement of data mining technology, personal information is often leaked inadvertently in daily life. American citizens with CIA work experience directly broke the news of the US “Prism Project” on the Internet. Furthermore, the US intelligence system conducted long-term monitoring of the private telephone calls of EU leaders. The advancement of network technology has not only brought about the convenience of information exchange but also aggravated the crisis of information security.

Information security generally refers to the unauthorized access of information systems and related information, which generally involves confidentiality, security, integrity, and authenticity of information and data. Information security is applied to all aspects of the country and society. It is not only applicable to commercial information security but also to personal information security and more applicable to national information security. Personal information in personal information security is generally defined in academia as the aggregate of personal public information and personal sensitive information. The concept of personal information security can be derived from its superordinate concept “information security;” that is, personal information encounters access operations by third-party entities that are not consented or authorized by the person, which destroys the corresponding integrity, authenticity, concealment, and security of personal information. Through the comparison of the two groups of concepts, it can be found that the subject of information security is broader and more diverse than the subject of personal information security. The subject of information security includes not only a large number of natural persons but also all commercial institutions and public institutions, and the focus of personal information security is mainly focused on the field of personal information.

The word “information” has a long history, and the word “xin” appeared in the Western Han dynasty more than 2,000 years ago. “Information” in everyday life usually refers to “sound or information,” but the definition of “information” is different in different fields. “Information” does not have a universal definition. Information can be expressed in many different forms, such as sounds, images, words, color, and temperature. There are various types of information, such as weather information, electronic information, personal information, and text information.

Information security can be understood in both narrow and broad senses. Information security in a narrow sense only reflects the security of information itself. In a broad sense, information security refers to protecting hardware and software related to information and the data on the information carrier (information system) from accidental or malicious attacks or leakage by ensuring the continuous and normal operation of the system and the uninterrupted provision of services in the network environment. The purpose is to ensure the integrity, confidentiality, authenticity, availability, irreversibility, and verifiability of information. Integrity means that data cannot be changed by unauthorized users and ensures the consistency of those data. Confidentiality indicates that the audience cannot understand the true meaning of information or cannot use confidential information. Availability means ensuring that legitimate user requests for information or resources are not unreasonably denied. Authenticity means being able to identify information from false sources and ensuring that the
source of the information is genuine. Irreversibility means preventing users from quitting their activities by having an effective mechanism in place. Verifiability provides a framework and tools for investigating emerging cybersecurity issues.

From the perspective of information security in a broad sense, the information security system consists of two parts: information carrier security and information content security. In the new information security model, information security issues are divided into three levels and four levels, and each level reflects the information security functions contained in the level. Information system security, information security, and information use security are three levels; four levels are physical security, operational security, data security, and content security.

A risk is the potential for a specific threat to exploit a vulnerability or set of vulnerabilities in an asset, resulting in the loss or damage of the asset, that is, the combination of the probability and consequences of a specific threat event.

Security risks are negative when they do not occur. The risk structure consists of five elements: origin, pattern, path, recipient, and outcome. Their interrelationships can be expressed as follows: one or more contexts, modes, paths, and receivers. Its meaning is explained in the following ways: The source of danger is called the source of the threat. The risk method is a method of identifying the source of the threat, which is called threat behavior. The risk path is the weak link of the threat source to implement the threat. The recipient of the risk is the recipient of the threat, i.e., property. The result of risk is the loss caused by exploiting a threat source, called impact. The concept of risk can be defined as exploiting a vulnerability to execute a threat to an asset. The relationship between assets, threats, vulnerabilities, and impacts is shown in Figure 4.

A security policy is the basis for designing, implementing, managing, and evaluating a security system. For specific information and network security, security policies determine which resources should be protected, how much should be spent, what actions should be performed, and which security enhancements should be obtained.

Risk assessment is an assessment of threats, impacts, and weaknesses of information and information processing facilities and the likelihood of the occurrence of the three. The risk evaluation is the procedure for identifying safety risks and severity levels. It shall use suitable risk evaluation tools, involving both qualified and measured methods, to prioritise the order of asset risk in terms of the level of controls.

Risk assessment is the practice of recognizing, controlling, mitigating, or neutralising possible security risks that might affect an operating information network at an affordable cost. Understand information security policies and manage risks using appropriate control objectives and implementation methods to avoid, deflect, or reduce risks to acceptable levels. The structure of the risk management process is shown in Figure 5.

Risk management must consider the balance between control cost and risk, which is a system, process, or method for reducing security risks. Residual risks are security risks that remain after security controls are implemented.

4. Information Security Problems and Countermeasures in the Era of Big Data

4.1. Big Data Information Security Issues. This section uses questionnaires to analyze people’s information security issues in the era of big data. Considering coverage, the survey population includes students, housewives, white-collar workers, and the elderly. The survey included respondents' information and daily experience, information security awareness, and use of security measures. 350 questionnaires were distributed, 330 were recovered, and 300 were valid. The distribution of male and female respondents is shown in Figure 6.

Among them, Figure 6(a) shows the number of male and female respondents and Figure 6(b) shows the proportion of male and female respondents. As can be seen from Figure 6, in the valid questionnaire, there were 170 male respondents, accounting for 56.67% and there were 130 women, accounting for 43.33% with a total of 300 people. It can be seen from the above data that the distribution of male and female ratios in this survey is relatively scientific, which can reflect the scientific nature of the sample in a balanced manner. The age distribution of respondents is shown in Table 1.

As can be seen from Table 1, among the valid questionnaires, the age distribution of the respondents is balanced. There were 40 people under the age of 25, accounting for 13.33%; 165 people between the ages of 25 and 35, accounting for 55%; 45 people between the ages of 35 and 45, accounting for 15%; 50 people over the age of 45, accounting for 16.67%. It can be seen from this that most of the people in this survey are young people, and this age group structure, because younger people learn more and use the Internet
more than older people. In terms of understanding, young people have more knowledge and acceptance than older people, so the age distribution of the respondents in this questionnaire is relatively scientific. The channels through which respondents provided information are shown in Figure 7.

Among them, Figure 7(a) shows the number of people who provide information through different channels and Figure 7(b) shows the proportion of people providing information through different channels. As can be seen from Figure 7, 230 people filled in real information when registering their e-mail addresses, accounting for 76.67%; 170 people filled in information during the job search process, accounting for 56.67%; 200 people filled in information when registering members, accounting for 66.67%. Figure 8 shows whether the respondents have lost personal items. Among them, Figure 8(a) shows the number of people with information loss and Figure 8(b) shows the proportion of information loss. As can be seen from Figure 8, mailboxes, WeChat QQ, etc., were stolen and communication equipment was attacked, and 200 people (66.67%) experienced this situation. In this case, information was lost, and the information of friends in the address book was also leaked. There are a small number of people whose information and friends’ information were leaked after their communication equipment was lost. 50 people experienced this situation, accounting for 16.67%. The information technology protection status of the respondents is shown in Table 1.

| Number of people | Proportion (%) |
|------------------|----------------|
| Less than 25     | 40             | 13.33          |
| 25–35            | 165            | 55             |
| 35–45            | 45             | 15             |
| More than 45     | 50             | 16.67          |

Table 1: Age distribution of respondents.

Figure 6: Distribution of the proportion of male and female respondents.

It can be seen from Table 2 that only 100 respondents set passwords to protect their information, accounting for 33.33%, 120 respondents installed firewalls, accounting for 40%, and 150 respondents could run antivirus software, accounting for 50%. Communication devices and storage devices are often used, and memory is occupied by small fragments of our lives. The information here is the epitome of everyone. If information is not encrypted, it would be like a transparent body, which would be displayed in front of others without any omission. Through the above data, the results obtained are not very optimistic. On the basic defense problem, only half of the people use it, and the others do not.

Through the above analysis, it is not difficult to find that the problems of information security mainly focus on the abuse of information and the information of the respondents cannot receive corresponding protection, so these problems should be optimized.

4.2. Optimizing Countermeasures for Big Data Information Security. This section builds on the questions raised in the previous section and optimizes them using IoT technology. In order to confirm the validity of the viewpoints presented in this section, this section uses the same data as the previous section to conduct a questionnaire survey on the information security of big data based on the Internet of things for analysis and comparison. The loss of big data information in the Internet of things is shown in Table 3.

It can be seen from Table 3 that based on the loss of big data information based on the Internet of things, 60 people were attacked on contact equipment, accounting for 20%, 9 people lost communication equipment, accounting for 3%, and 15 people lost storage equipment, accounting for 5%. Compared with before, the number of people who were attacked on contact equipment decreased by 140 with a total decrease of 46.67%, the number of people who lost communication equipment was decreased by 41 with a decrease of 13.67%, and the number of people who lost storage equipment was decreased by 85 with a decrease of 28.33%. It can be seen from the data that the probability of big data information loss based on the Internet of things is significantly lower than that without Internet of things technology, indicating that the addition of the Internet of things is more stringent in the management and control of big data.
information. The big data information protection of the Internet of things is shown in Table 4.

It can be seen from Table 4 that 260 people set passwords in communication devices and storage devices, accounting for 86.67%, 200 people installed firewalls, accounting for 66.67%, and 230 people ran antivirus software, accounting for 76.67%. Compared with before, the number of people who set a password increased by 160, with a total increase of 53.34% and the number of people who installed firewalls and ran antivirus software both increased by 80, with a total increase of 26.67%. It can be seen from the above data that the protection of big data information under the Internet of things has been significantly improved.

The comparison of the above data showed that the big data information security technology based on the Internet of things proposed in this section is highly feasible and is of great help to today’s information security development.

5. Conclusion

With the rapid progress of traditional Internet technology, big data technology, and IT industry, Internet technology has evolved at a rapid pace, and all fields of life have entered the big platform of the Information Age. Especially in recent years, network technology has expanded to broadband, and many new services such as e-commerce, instant messaging, online social networking, and mobile payment based on big data have entered people’s daily lives. With the rapid development and prosperity of big data, various information...
security phenomena such as the theft of personal privacy information on mobile phones, the dissemination of malicious codes, and fraudulent information content have also attracted public attention. Network security incidents have gradually shifted from computers to mobile terminals, and the leakage of sensitive information has become more subtle and frequent. Big data security has become a major issue for information solutions. Therefore, through the research on the Internet of things, this paper put forward practical suggestions for big data information security management, which is of great intellectual and empirical relevance.

**Data Availability**

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

**Conflicts of Interest**

The author declares that there are no conflicts of interest.

**References**

[1] J. Lin, “Towards a fault-tolerant, scheduling methodology for safety-critical certified information systems,” *Journal of International Technology and Information Management*, vol. 27, no. 3, pp. 5-6, 2019.

[2] J. Liu and C. Z. Hu, “Application of information technology in active safety control for construction machine,” *Procedia Engineering*, vol. 174, no. Complete, pp. 1182–1189, 2017.

[3] C. I. Nitsche, “Promoting safety culture: an overview of collaborative chemical safety information initiatives,” *Journal of Chemical Health and Safety*, vol. 26, no. 3, pp. 27–30, 2019.

[4] J. Wang, H. Liang, H. Kang, and Y. Gong, “Understanding health information technology induced medication safety events by two conceptual frameworks,” *Applied Clinical Informatics*, vol. 10, no. 01, pp. 158–167, 2019.

[5] L. McEwen, R. Stuart, E. Sweet, and R. Izzo, "Baseline survey of academic chemical safety information practices," *Journal of Chemical Health and Safety*, vol. 25, no. 3, pp. 6–10, 2018.

[6] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging internet of things marketplace from an industrial perspective: a survey," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 4, pp. 585–598, 2015.

[7] S. E. Collier, "The emerging internet of things: convergence of the smart grid with the internet of things," *IEEE Industry Applications Magazine*, vol. 23, no. 2, pp. 12–16, 2017.

[8] R. P. Smruti and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, no. 1, pp. 1–10, 2017.

[9] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.

[10] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[11] B. B. Zarpeia, R. S. Miani, C. T. Kawakani, and S. C. de Alverenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, no. Apr, pp. 25–37, 2017.

[12] R. Li, Y. V. Chen, C. Sha, and Z. Lu, "Effects of interface layout on the usability of In-Vehicle Information Systems and driving safety," *Displays*, vol. 49, no. sep, pp. 124–132, 2017.

[13] V. Oliveira and G. D. Santos, "Information technology acceptance in public safety in smart sustainable cities: a qualitative analysis," *Procedia Manufacturing*, vol. 39, no. 4, pp. 1929–1936, 2019.

[14] J. Chen, Y. Liang, J. Zhang, and G. Qi, "The online social network and user innovation in the context of an online innovation platform," *Journal of Organizational and End User Computing*, vol. 33, no. 6, pp. 1–27, 2021.

[15] C. Hiar, "In reversal EPA limits information on safety reviews," *Greenwire*, no. jan 10, pp. 1–3, 2018.

[16] K. A. Ogudo, D. Muwawa Nestor, O. Ibrahim Khalaf, and H. Daei Kasmaei, "A device performance and data analytics concept for smartphones’ IoT services and machine-type communication in cellular networks," *Symmetry*, vol. 11, no. 4, pp. 593–609, 2019.

[17] A. Burd, "How to share health and safety information through building information modelling," *Proceedings of the Institution of Civil Engineers. Civil Engineering*, vol. 171, no. 4, p. 149, 2018.

[18] A. S. Kesselheim, S. A. Mccgraw, S. Z. Dejene et al., "Patient and physician perceptions of drug safety information for sleep aids: a qualitative study," *Drug Safety*, vol. 40, no. 6, pp. 531–542, 2017.

[19] H. Chimowitz, M. Gerard, A. Fossa, F. Bourgeois, and S. K. Bell, "Empowering informal caregivers with health information: opennotes as a safety strategy," *Joint Commission Journal on Quality and Patient Safety*, vol. 44, no. 3, pp. 130–136, 2018.

[20] A. K. Singh, X. Liu, H. Wang, and H. Ko, "Recent advances in multimedia security and information hiding," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, Article ID e4193, 2021.

[21] M. Soni, Y.K. Barot, and S. Gomathi, "A review on privacy-preserving data preprocessing," *Journal of Cybersecurity and Information Management*, vol. 4, no. 2, pp. 16–30, 2020.

[22] Z. Longchao, X. Jianjun, and Y. Limei, "Research on congestion elimination method of circuit overload and transmission congestion in the internet of things," *Multimedia Tools and Applications*, vol. 76, no. 17, pp. 18047–18066, 2017.

[23] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[24] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in internet of things (IoT) using economic analysis and pricing models: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2546–2590, 2016.