Exploration of Network Information Security Technology and Prevention in the Digital Age

Hongfei Xiao[1, 2*]

[1] School of Information Engineering, Chuzhou Polytechnic, Chuzhou, 239000, Anhui, China
[2] Computer College of Chongqing University, Chongqing, 400044, China
[*]Corresponding Author.

Abstract:

Since the digital age, the virtual and open nature of network information technology has led to frequent information security problems, such as hidden dangers of information leakage, risk of cyber attacks, insufficient audit supervision, backward security technology, etc. Therefore, how to protect users' information while developing information technology has become a big problem. In this paper, in order to protect the data security and privacy in the digital age, the problems existing in the current application of information technology were analyzed, and the solutions to the information security problems were put forward, such as strengthening the prevention of network information security technology by putting an end to the hidden dangers of information leakage, preventing the risk of network attacks, strengthening audit supervision, and cultivating security technical talents.

Keywords: The digital age, Cloud computing, Big data, Information technology, Security protection.

I. INTRODUCTION

In the digital era, with the rapid development of science and technology, information technology has been widely used in the financial, medical, media, education and other industries, which has profoundly changed people's life, work, entertainment and other ways, such as sweeping robots, unmanned supermarket and so on, which are the embodiment of the application of information technology in social production and life. New generation information technologies such as 5G, artificial intelligence, Internet of Things, big data, cloud computing, blockchain, etc. are rapidly emerging and gradually maturing. Information technology has caused extensive and profound changes in the world, bringing new development opportunities and challenges to the information construction, especially the security issues, because information technology under non-security protection will have a negative impact on the user's personal privacy. In the background of the digital age, the digital revolution is no longer for "machine", but for "information". To solve the problem of information security in the future, it is necessary to strengthen the research on information security technology and prevention.

II. INFORMATION SECURITY TECHNOLOGY IN THE DIGITAL AGE

The rapid development of network information technology has fully integrated into social production and life, and digitalization has also become one of the main features of the 21st century. Not only have people's ways of obtaining information, communicating with others, organizing activities and obtaining services undergone earth-shaking changes, but individuals and groups separated from different geographical spaces and time zones around the world are increasingly interconnected and interact with each other at high frequency, and all aspects of economic development, social life and government governance have entered the digital age. "ABC", which is composed of Artificial Intelligence, Big Data and Cloud Computing, has become a recognized trend of information technology. In addition, there are information technologies such as the Internet of Things, blockchain and 5G, which have led to a new round of information technology trends and triggered a new industrial revolution and technological revolution, making the business model and interactive mode of information technology industry changed fundamentally.

2.1 Artificial Intelligence (AI)

Artificial intelligence (AI) is a new technological science. Its theoretical methods and technological systems can be used to simulate human intelligence. As a branch of computer science, it is mainly used in the fields of language or image recognition, robotics and natural language processing. Formally proposed in 1956, AI as a discipline has been defined as the three cutting-edge technologies in the 21st century together with genetic engineering and nanoscience with the continuous development and growing maturity of the discipline's theory and technology. According to the *China Internet Development Report* (2021) released by the Internet Society of China on July 13, 2021, the scale of the artificial intelligence industry maintained a steady growth in 2020, reaching 303.1 billion yuan, a year-on-year growth of 15%, slightly higher than the global average growth rate.

2.2 Big Data

Big data, also known as mass data, refers to information that can be retrieved, managed, processed, and sorted out in a reasonable time by using all data for analysis and processing, so as to help enterprises make more active business decisions [1]. IBM has proposed the 5V features of big data: Volume, Velocity, Variety, Value and Veracity [2]. Big Data Analysis is designed for IT management, which applies the concept of data to the data generated by IT operation tools to provide data support for IT management software suppliers to solve business problems. It enables enterprises to combine real-time data flow analysis with historical relevant data and discover the models they need to help anticipate and prevent future operational disruptions and performance issues, leverage big data to track and document network behavior, easily identify business impacts, and gain insight into big data for valuable users.

2.3 Cloud Computing

Cloud computing, also known as grid computing, is a kind of distributed computing, which refers to the process that huge data processing programs are decomposed into numerous small programs through the "cloud" of the network, and then these small programs are processed and analyzed by a system composed of multiple servers to obtain results and return them to users [3]. As a big data platform based on the internet and computer, it integrates and calculates personal data, processes data in a few seconds, improves the accuracy of research results and the utilization rate of data results, and realizes the powerful network service function. In the context of the digital age, cloud computing's intelligent, fast data processing function has been widely used. In the development of enterprises, cost problems can be effectively controlled through data analysis, so as to plan the future development direction of enterprises and maximize the benefits of enterprises. In daily life, people's living habits can be obtained by classifying and integrating a large amount of data, such as the use of various robots, which brings great convenience to daily life.

2.4 Internet of Things (IoT)

The Internet of Things, fully called "the Internet where everything is connected", is an extension and expansion of the original Internet, which combines the Internet with various information sensing devices to realize the interconnection of people, computers and things in order to overcome the differences of time and space. Specifically, the information sensing devices and technologies of the Internet of Things include radio frequency identification technology, global positioning system, information sensors, etc., which monitor and connect objects in real time through the Internet, and then collect all kinds of required information. In this process, the real-time connection between objects and objects and between objects and people is established, and finally the networked and intelligent management is realized. Under the background of the digital age, the Internet of Things has been applied to education, national defense, finance, industry, agriculture, environment, service, transportation and other fields. It has greatly improved the efficiency of the industry by making scientific and rational use and allocation of resources through intelligent, information-based and precise management. On July 13, 2021, the Internet Society of China released *China Internet Development Report* (2021), which pointed out that the scale of China's ground objects networking market reached 1.7 trillion yuan.

2.5 Blockchain

In the field of information technology, blockchain, as a new application mode of computer technology, mainly includes information technology such as encryption algorithm, point-to-point transmission and distributed data storage. It solves the problem of information asymmetry by establishing distributed shared account books and databases so as to achieve the result of concerted action by multiple subjects. Blockchain has a wide range of connotations and applications, not only involving the Internet and computer programming technology, but also covering the fields of cryptography and logic. The information and data stored in the blockchain are characterized by "de-centralisation", "unforgeability",

"full-course marking", "traceability", "openness and transparency" and "collective maintenance", thus ensuring the "honesty" and "transparency" of the blockchain and laying a foundation for creating trust in the blockchain. In the digital age, blockchain has broad application prospects and is widely used in insurance, finance, public services and other fields. [4].

2.6 5th Generation Mobile Communication Technology (5G)

5G stands for "The Fifth Generation Mobile Communication Technology", which has the outstanding characteristics of high speed, low time delay and large connection. As a new generation of network infrastructure, it realizes man-machine interaction through broadband mobile communication technology. The rapid development of mobile Internet has promoted the integration of information technology into all aspects of social life, profoundly changing people's communication and even the whole way of life. With the development of 1G, 2G, 3G and 4G era, every technological progress has greatly promoted the industrial upgrading and economic and social development. The wide application of 5G technology in all walks of life in the economy and society can not only solve people-to-people communication problems, provide services including virtual reality, VR technology and mobile cloud, but also solve people-to-things and things-to-things communication problems, and meet the application requirements of Internet of Things, such as mobile medical care, car networking, smart home, industrial control and environmental monitoring. Therefore, 5G has become a key new infrastructure leading the social economy to digital, networked and intelligent transformation.

III. CURRENT SITUATION AND PROBLEMS OF NETWORK INFORMATION SECURITY

In the digital age, the rapid development of network information technology has brought great changes in economy and society, greatly promoted the intelligent and information development of human society, and increased the transmission rate of information unprecedentedly. However, the network security problems that followed have also produced many adverse social impacts. With the technological progress, the Internet architecture of software is becoming more and more complex and diversified. The data and information that the traditional network security analysis system can store and process can't be effectively protected by the original device network security defense means due to technical limitations. The main problems are:

3.1 Hidden Danger of Information Leakage

In the digital age, people are facing greater information security challenges, the most likely one is how to solve the problem of security leakage in the process from user data to personal enterprise data account information. 5G can transmit data faster than the transmission technology of 4G network, but it also brings problems. On the one hand, 5G users can establish inaccessible links with other users on a large scale and quickly. The more users, the greater the risk of security. On the other hand, personal network data are easily obtained but difficult to be traced, and it is easy to lose and steal personal business privacy and confidential data, resulting in frequent information disclosure such as personal account data and privacy

[5]. Network technology is characterized by remoteness and virtualization, and has potential security risks of information leakage. According to the survey, more than 70% of enterprises and institutions are troubled by the problem of information confidentiality, and some even give up the application of cloud services in order to avoid the economic losses caused by information leakage. With the development of digital age, the requirements for data confidentiality are getting higher and higher. How to encrypt and isolate high-security data is one of the hot research issues at present.

3.2 Risk of Cyber-Attack

Along with the development of information technology and means, the risk of cyber-attack is also escalating. First, the risk of network virus spread and attack is escalating. Traditional network viruses steal users' information and data through self-replication, and even delete personal data stored in computers by themselves, resulting in data loss. By remotely operating new network viruses, criminals send links through chat tools such as SMS and WeChat, in order to steal user information and transfer user property. Moreover, the popularity of mobile phones is causing more and more harm. Second, the risk of hacking is escalating. Traditional network hackers steal users' private information by invading their computer systems to obtain illegal gains, while new network hackers steal public information by attacking public systems, which affects social order [6]. Although the digital age provides various types of network attack systems with faster, larger and higher capacity for network users, there are also risks of various types of network attacks.

3.3 Insufficient Audit Supervision

In the digital age, there are a variety of information technologies, among which the most influential one is the "ABC" composed of artificial intelligence, big data and cloud computing. For example, in cloud computing, users in the outsourcing state can't directly manage data information which however are managed by cloud computing service providers, leading to serious security audit risks. On the one hand, because the service providers can't guarantee the transparency and security of security audit information when they supply security audit information, once the system is illegally invaded, and problems such as data loss or damage occur, the service providers may make up data at will in order to avoid responsibility. At the same time, it is also prone to the problem of insufficient information transparency, and passing the buck often in the process of accountability when information security accidents occur. On the other hand, the continuous development of network information technology has promoted the updating of technical means of network crime, but the relevant laws and regulations are not perfect enough to form a perfect information security supervision and management system. The existing information security protection system has just started in some areas, and its implementation is not sufficient enough, resulting in great pressure on information security prevention.

3.4 Backward Security Technology

Information security technology and prevention is an important part of information construction. As

the application field of information technology continues to expand, most government departments and enterprises and institutions have added security facilities in order to ensure information security, but the information security problem is still very serious. On the one hand, the lack of information security technology personnel makes the implementation of modern information security technology inadequate; On the other hand, network attacks and virus types continue to develop differently, but data security technologies cannot be updated simultaneously [7]. The development of information technology has greatly improved the speed of information dissemination. However, due to the open environment of the network, the Internet is full of bad information, which creates public opinion by publishing false information, guides and incites the public's emotions, and affects social stability and even destroys the stability and unity of the country. Backward security technology has never been able to solve the problem of bad information dissemination.

IV. STRATEGIES FOR SOLVING INFORMATION SECURITY PROBLEMS

Information technology is widely used in all walks of life, which is the development trend of the digital age. In order to adapt to the development of the digital age and the technological change of the digital revolution, the network information security technology and prevention must be integrated into the information technology in order to better maintain the network information system and provide technical support for its safe and orderly operation. Under the background of the digital age, the traditional information security technology cannot match the information security demand at the present stage. Only by constantly upgrading the information security technology and strengthening the prevention can the information security be fundamentally guaranteed [8]. Specifically, there are mainly the following strategies:

4.1 Putting an End to Hidden Dangers of Information Leakage

On the one hand, illegal access should be strictly restricted. The openness of the Internet leads to the endless emergence of illegitimate interests by stealing data and information. Therefore, the identification of users should be strengthened, for example, through various ways such as setting password, mobile phone or email binding, ID card real-name authentication, etc. At the same time, the access rights of users should be strictly controlled. Users with suspicious identities should be strictly prohibited from logging in. Once the service platform is illegally invaded, other users should be warned immediately to strengthen data information management to prevent data theft. On the other hand, data management should be strengthened. Although big data and cloud computing are fast and flexible in information collection and processing, they are prone to hidden dangers, data theft and cloud data loss. Therefore, data classification should be done well during data processing, especially for important data and key data. Backup must be done well. Important data can be backed up while being stored in the cloud. Key data and core data should be kept in the cloud as far as possible to reduce the risk of information leakage and ensure the application safety and stability of data information.

4.2 Preventing the Risk of Cyber-Attack

The main practices are: Firstly, constantly improving the anti-virus intrusion technology, including static and dynamic methods. Because the static anti-virus technology is relatively backward and cannot meet the current network information security requirements, most of the current information systems adopt dynamic anti-virus technology to conduct a comprehensive monitoring of the information system. Once an illegal intrusion is found, it can be timely warned and intercepted, thus protecting the information to the maximum extent [9]. Second, strengthening the terminal intelligent firewall technology. As one of the core security networks in network information system, firewall is mainly used for information filtering, running in the external network information environment and internal information environment. The firewall with strong attributes can realize the free transformation of the network, and the intelligent firewall can even monitor and analyze the system, complete the detection work in the background, analyze the user's behavior and protect the data while reducing the interference to the user's operation, prevent illegal personnel from intercepting the data pertinently, and prevent the network attack risk to the maximum extent [10]. Thirdly, enhancing information security awareness, such as not opening strange SMS, WeChat messages and e-mails, or downloading programs with unknown intentions at will, downloading software from regular websites and browsers, using complicated passwords as much as possible and changing passwords regularly, using self-care network proxy servers to set up proxy servers, hiding IP addresses, effectively protecting IP addresses, preventing network attacks as much as possible and ensuring information security.

4.3 Strengthening Audit Supervision

In order to ensure the security and stability of applications, service providers of big data or cloud computing platforms should be subject to the audit of relevant departments before providing services to users, including hardware settings, software applications and security management mechanisms. At the same time, they should regularly report audit information to users, and add an alarm device during platform construction, so that problems can be found and solved in time. When signing outsourcing contracts, they should make clear their responsibilities, so as to reasonably ascertain where the responsibility lies for problems such as user information loss. Relevant management departments should strengthen the supervision of the network platform, constantly improve relevant systems and laws and regulations, especially those of two-way cross-border information transmission. Government departments, enterprises and institutions should formulate corresponding information security management measures based on their own technical specifications and the security level of internal information, strictly implement them, and accept the audit, supervision and management of the information department [11].

4.4 Training Security Technical Personnel

In order to build a network power, it is necessary to strengthen the training of information security technical personnel, build an information technology team with strong business ability and high professional quality, and continuously strengthen and update the advanced information security technology

education. With the continuous upgrading of network attack means, information security technology also keeps pace with the times. Commonly used technologies mainly include identity authentication technology, access control technology, intrusion detection technology, new encryption technology and so on [12]. In order to manage information security well, relevant staff should continuously improve their own business capabilities, pay attention to improving their own operation technology, especially advanced technology, accurately identify information security issues and take corresponding measures. Therefore, the management organization and the employing unit should consciously cultivate information security technical personnel and scientifically and reasonably formulate the training plan. In particular, colleges and universities should closely meet the market demand and the needs of the country, and cultivate excellent information technology talents for the society in the field of information technology.

V. CONCLUSIONS

In the digital age, the information technology represented by artificial intelligence, big data, cloud computing, Internet of Things, blockchain and 5G has been continuously developed and applied in all aspects of people's lives, which has extensively and profoundly changed social production methods such as industrial forms, business models and interactive ways. The following network information security problem has become a normal problem of information technology. Network security is always facing new attacks and challenges, mainly including hidden dangers of information leakage, network attack risks, inadequate audit supervision, backward security technology and other issues. Network security technology and prevention is a long-term and endless work, which requires both technical and management means. It can effectively protect network information security by eliminating hidden dangers of information leakage, preventing network attack risks, strengthening audit supervision and training security technicians.

ACKNOWLEDGEMENTS

REFERENCES

[1] Zhou Lifeng, Liu Wen, Zhang Zhizhong. Role of Cloud Computing in Informatization of Water-conservancy Scientific Research. Journal of Yangtze River Scientific Research Institute, 2014, 31 (09): 110-114.

[2] Xiao Zigan, Chen Jingyou, Fu Shi. Overview on the Development of Intelligent Transportation System in the Context of Big Data. Software Guide, 2017, 16 (01): 182-184.

[3] Gao Yuan, Wu Chang'an. Study of Informational Security Question under the Cloud Computing. Information Science, 2015, 33(11):48-52.

[4] He Yuanxiang, Xia Tian, Shi Baoming. Research on Key Technologies of Blockchain. Journal of Lanzhou University of Arts and Sciences (Natural Science Edition), 2020, 34 (06): 92-98.

[5] Cao Dayuan. Intrusion Detection Technology. Beijing: People's Posts and Telecommunications Publishing House, 2013.

[6] Hu Jianwei. Network security and confidentiality. Xi 'an: Xidian University Publishing House, 2003.

[7] Li Jing. "Prism" under the Refraction of Network and Information Security Challenges and Strategic Thinking. Information Theory and Practice, 2014, 37 (04): 48-52.

[8] Sherman J, Arampatzis A. Social engineering as a threat to societies. The Cambridge Analytic Case, 2018 (7).

[9] Sun Hongmei. Research on Enterprise Information Network Security in Big Data Environment. Software Guide, 2015(11): 4-5.

[10] Thomas E, Zaigham M, Ricardo P. Cloud computing concept, technology and architecture. Gong Yili, He Lian, Hu Chuang (translators). Beijing: Mechanical Industry Press, 2014.

[11] Xu Cheng, Research on Network Attack Prevention Methods for Enterprise Information Security, Journal of China Academy of Electronics and Information Technology, 2020 (5): 483-487.

[12] Zeng Zhongliang. Enterprise Information Security in the Era of Big Data. Network Security Technology & Application, 2014 (08): 137-138.