

# Research on Information Communication Network Security Under the Background of Big Data

Xiaoying Chen

Guangzhou City University of Technology, Guangzhou, China

**Keywords:** Big Data, Information and Communication Networks, Security Policy.

**Abstract:** At present, the rapid development of big data technology has a wide impact on all walks of life. This study is based on the information communication network security management under the background of big data. By analyzing the background and importance of network security, this paper aims to explore the information and communication network security management strategy, research and formulate information and communication network security risk management strategy and network security protection strategy in view of relevant issues, so as to cope with the security challenges in the context of big data. The purpose of this study is to improve the security of information and communication networks and provide important reference for the security management of information and communication networks in the era of big data.

## 1 INTRODUCTION

Under the background of big data, the information communication network security management strategy has attracted more and more attention. With the continuous development and application of technology, the problem of network security becomes more and more prominent, and the protection of information and communication network security becomes particularly important. The purpose of this study is to improve the security of information communication network by studying the strategy of security management. At present, the rapid development of big data technology has a wide impact on all walks of life. The extensive collection and analysis of big data enables businesses to gain more information about users and markets. However, it also raises the concern of information communication network security. Various types of attacks are becoming more common, such as malware and hacking. It is imperative to study the strategy of information communication network security management. The significance of this study is to provide in-depth research and practical guidance for information communication network security management strategies. In the context of big data, the importance of network security is more prominent. Through the results of this study, it provides an important reference for the information communication network security management in the

background of big data, and provides a foundation for further research and practice.

## 2 BIG DATA DEVELOPMENT CHALLENGES INFORMATION AND COMMUNICATION NETWORK SECURITY

The development of big data is currently in a stage of rapid growth, which is characterized by mass, high speed, diversification and real-time, and has a profound impact on all walks of life. With the continuous development of computer network technology, the problem of information communication network security also appears. These problems include business secrets being leaked, users' personal information being resold by criminals, and even high-level hackers invading national networks and endangering national network information security. These problems lead to the leakage of personal privacy and the theft of intellectual property rights of enterprises, which brings interference to the development of science and technology, and also puts higher requirements on information protection technology. According to relevant surveys, the main risk factors for data loss are as follows, as shown in Fig. 1:

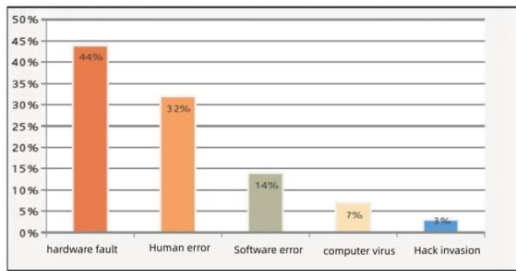


Figure 1: Main factors of data loss risk.

First, the development of Big data has brought many new impacts on the security of information and communication networks. The traditional security protection strategy will appear powerless in the face of Big data. Because of the huge amount and diverse types of Big data, traditional security protection measures cannot meet their requirements for efficient processing and protection. At the same time, the real-time nature of Big data requires that the information communication network security management strategy must be capable of rapid response and real-time monitoring. In the context of Big data, information and communication network security is faced with multi-level and all-round threats and attacks. Firstly, the virtuality and boundary ambiguity of cyberspace complicate the network security situation. With the rise of cloud computing and the Internet of Things, more and more devices and systems are connected to the network, providing more opportunities and entrances for hackers to attack. In addition, the increasing scale and complexity of information and communication networks have made security management tasks more difficult. The information communication network in the context of Big data contains huge data flow and massive information, and the traditional security management methods can no longer meet the needs of large-scale networks. Moreover, the continuous innovation and evolution of network attack technology have made the network security situation even more severe. Hackers have adopted more covert and advanced attack methods to bypass traditional security measures, posing a huge threat to network security. Therefore, we need to use advanced technical means and innovative ways of thinking to deal with information network security management in the context of Big data, and ensure the security and stability of the communication network.

Secondly, the rapid development of information and communication networks and the wide application of Big data have brought new challenges to network security. With the development of Big

data technology, personal privacy and data security are facing huge risks. The collection, storage, transmission and processing of Big data may reveal users' private information. The centralization and sharing of Big data makes personal privacy exposed and abused, and data security also faces more threats. In addition, with the rapid growth of Big data, the scale and complexity of network attacks are increasing, and the risk of network security is becoming more serious. Therefore, we need to study and formulate information communication network security management strategies against the background of Big data to protect personal privacy and data security.

### 3 INFORMATION AND COMMUNICATION NETWORK SECURITY MANAGEMENT STRATEGIES IN THE CONTEXT OF BIG DATA

In response to the above challenges, we need to research and develop information and communication network security risk management strategies and network security protection strategies. The network security risk management strategy includes methods and measures to identify, evaluate, and control communication network security risks. By identifying the sources and potential threats of network security risks, we can develop targeted risk control measures to minimize the impact of security risks on information and communication networks.

The security protection strategies for information and communication networks include establishing a security protection system, strengthening network boundary defense, and applying encryption technology. By establishing a comprehensive security protection system. At the same time, strengthening network boundary defense and applying encryption technology can effectively prevent unauthorized access and data theft, ensuring network security.

#### 3.1 Information and Communication Network Security Risk Management Strategy

With the rapid development of Big data technology, the security situation of information and communication networks has become increasingly severe and diversified, bringing unprecedented

challenges to network security management. The study of information and communication network security management strategies has become particularly important, as it is of great significance for protecting network security and preventing network attacks.

Network security risk management strategy is a key link in information and communication network security. In the Big data environment, network security risks are highly complex and uncertain. Therefore, in terms of network security risk management, it is necessary to strengthen the identification, evaluation, and monitoring of network security risks, and develop corresponding response measures to reduce the probability and impact of risks. The network security risk management strategy should be comprehensive, scientific, and able to adapt to the rapid changes in the current network security situation. Firstly, the management of network security risks should start with risk identification and assessment. This means accurately identifying and evaluating potential network security threats in order to take timely measures to reduce risks. Secondly, network security risk management should focus on monitoring and controlling risks. By establishing effective monitoring and detection mechanisms, timely detection and response to network security incidents can be achieved to minimize potential losses. In addition, information and communication network security risk management should also focus on risk response and emergency response. When network security incidents occur, corresponding measures should be taken in a timely manner to respond and handle them, in order to reduce damage to network security.

### 3.2 Security Protection Strategies for Information and Communication Networks

Network security protection strategies are an important aspect of ensuring the security of information and communication networks. In the context of Big data, the security situation of information and communication networks is more severe, so effective network security protection strategies need to be developed to deal with various potential threats. In terms of network security protection, technical means such as network intrusion detection systems, firewalls, data encryption, and access control can be utilized to ensure network security.

#### 1) Establishing a Sound Network Security System is the Foundation of Network Security Protection

This system includes the security protection of network hardware devices, network software, and network data. For the security protection of hardware devices, technical means such as firewalls and intrusion detection systems can be used to monitor and protect the security of the network. For software security protection, potential security vulnerabilities can be discovered and repaired in a timely manner through methods such as vulnerability scanning and security detection. For data security protection, encryption technology, access control, and other means can be used to ensure the confidentiality and integrity of data.

(a) Data encryption technology. In order to ensure the security and stable performance of computer data communication networks, encryption technology must be combined with encoding to protect the security of data through specific keys. Encryption technology typically consists of two aspects: keys and algorithms. A key is a special calculation method used to encode and decode data. The algorithm combines the collected information with the key to transmit data in the form of ciphertext. With the rapid development of information technology, encryption technology continues to improve and improve. Especially with the increasing emphasis on data security, encryption technology has been widely applied in the process of data transmission.

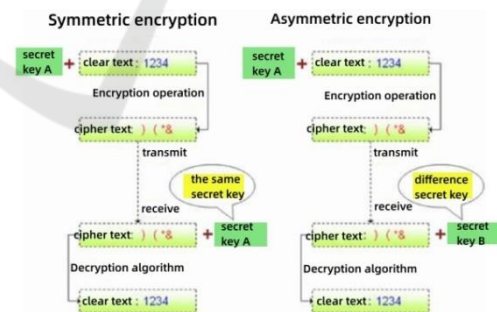


Figure 2: Encryption type and characteristics.

Generally, nodes in the process of data exchange privacy steganography encryption in Big data mobile communication networks can sense information within the same time and region. In the protocol layer, the redundancy of Big data mobile communication network data cannot be reduced or eliminated. To better solve this problem, all node data can be aggregated to the physical layer, compressed, and then sent to different servers

separately. In order to simplify the operation, Distributed source coding technology can be introduced in the physical layer. This technology can effectively solve the compression problem between non connected sources, and nodes can decode when the code is known. Use Fig.3 to provide a detailed description of the process of independent decoding and joint decoding.

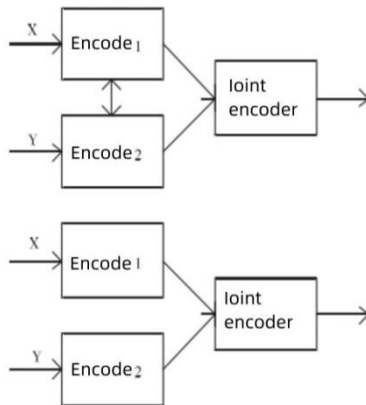


Figure 3: Independent decoding and joint decoding processes.

(b) Firewall technology. This is an effective way to improve security policies by possessing strong data security protection capabilities. Its main function is to isolate communication between networks and implement access restrictions. Simply put, it allows information that is accessed by data to pass through, while isolating information that is not allowed to be accessed. By using firewall technology, malicious access can be maximally prevented. If firewall technology is not set up, data may be accessed arbitrarily, making it impossible to ensure information security. Once data is maliciously tampered with or leaked, the consequences will be unpredictable. In the era of Big data, firewall technology is like a "security door" for data security, so it is highly valued.

2) Establishing a Comprehensive Network Security Monitoring and Warning Mechanism is also an Important Means of Network Security Protection.

By establishing a network security monitoring system, network traffic, abnormal behaviors and security events can be monitored in real time, and alerts can be sent in time. At the same time, Big data analysis technology can also be used to predict and warn network security events, and corresponding security measures can be taken in time to prevent network security threats.

3) Timely Updates and Upgrades of Information and Communication Network Security Technology are also Key to Network Security Protection.

Network security technology is constantly developing and evolving, and only by timely understanding and adopting the latest security technologies and protective measures can we better respond to constantly changing threats. Therefore, organizing network security experts to participate in the research and promotion of security technologies, as well as timely updating and upgrading network security technologies, plays an important role in enhancing network security protection capabilities.

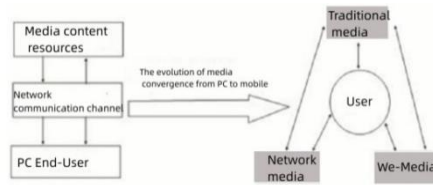


Figure 4: Integrated network technology.

#### 4 CONCLUSION

Aims to improve the security of information communication network by studying the security management strategy of information communication network in the context of Big data. We have proposed network security risk management strategies and network security protection strategies for the Big data environment to meet the challenges of information and communication network security. To sum up, the information and communication network security management strategy is increasingly important in the context of Big data. Network security risk management and network security protection are two key aspects of information and communication network security management. Through scientific and reasonable network security risk management strategies and network security protection strategies, network security capabilities can be effectively improved, network security risks can be reduced, and network security can be protected. In the context of Big data, the research on information communication network security management strategy will provide important theoretical guidance and practical experience for network security. Network security protection strategy is an important means to ensure the security of information communication network in the context of Big data. By establishing a sound network security system, establishing comprehensive



network security monitoring and warning mechanisms, and timely updating and upgrading network security technologies, the security protection capabilities of information and communication networks can be effectively improved to cope with various potential security threats.

This article proposes the following points for future research directions and practical suggestions. First of all, it is recommended to further study the implementation effect and influencing factors of the information and communication network security management strategy in the context of Big data to optimize the network security management strategy. Secondly, it is recommended to strengthen training and education on information and communication network security management strategies, and improve the security awareness and skill level of relevant personnel. In addition, we also call for strengthening international cooperation, jointly addressing the challenges of network security in the era of Big data, and promoting the development and application of information and communication network security.

## REFERENCES

- Wang Tao, discussion on network security defense measures in the context of Big data era [J], *Network Security Technology and Application*, 2022 (08): 56-57.
- Tang Xinmei, Qin Kaixian, privacy steganography encryption for data exchange of Big data mobile communication network [J] *Computer Simulation*, 2022, 39 (06): 403-407
- Li Pengju, a brief analysis of the information and communication network security management strategy in the context of Big data [J] *Digital Technology and Applications*, 2021,39 (05): 184-186
- Dai Xunan, Shen Youxiang, Pan Dan, Research on Information and Communication Network Security Management Strategy in the Context of Big data [J]. *Internet plus Communication*, 2021:7-9
- Wen Wei, Research on Information Communication Data Encryption Technology under Big data [J]. *Electronic Technology and Software Engineering*, 2021:257-258
- Ye Lijia, Research on Information Communication Network Security Management Strategy in the Context of Big data [J]. *Digital Technology and Application*, 2018: 178-179
- Yang ChunYan, Ling Ying, Li Xin. Research on Information Encryption Algorithm under the Power Network Communication Security Model [J]. *Journal of Physics: Conference Series*, Volume 1852, 2021(03). <https://doi.org/10.1088/1742-6596/1852/3/032007>
- Liu Lei, Research on Information Communication Network Security Management Strategy in the Context of Big data [J] *Network Security Technology and Applications*, 2022 (08): 57-59
- Du Meiyuan, Application of information communication network security management and control based on big data technology [J]. *International Journal of Communication Systems*, 2020(05). <https://doi.org/10.1002/DAC.4643>
- Chen Yanhua, Research on Network Application Service Quality Monitoring Based on Big data Technology [D]. *Master's Thesis of Xiamen University*, 2018
- Zhang Ying, Research on Archives Informatization Construction in the Context of Big data [J] *Heilongjiang Archives*, 2021 (03): 210-211