**International Journal of Information Technologies and Systems Approach**
Volume 16 • Issue 2

# Computer Network Information Security and Protection Strategy Based on Big Data Environment

Min Jin, State Grid Chongqing Electric Power Company Information Communication Branch, China*

## ABSTRACT

This paper proposed a study on computer network information security and protection strategy based on a big data environment. The research purpose was to use big data technology to network information security protection technology and seek more efficient network information protection technology. The algorithm proposed in this article was a time-series network detection algorithm based on big data, which could improve the early warning rate of abnormal network information, reduce the early warning time, and improve the detection accuracy and interception rate of virus information. The results of this study could effectively show that big data technology had excellent performance in computer network information security protection, which also led to an advanced reform path for future network information security protection technology.

## KEYWORDS

Big Data Environment, Computer Network Information Security, Cyber Attacks, Network Protection Policy

## INTRODUCTION

In recent years, both life and production have been networked, bringing humankind many conveniences. However, everything has advantages and disadvantages. The growing network information security crisis has had a great security impact on mankind. In the informatization process, addressing computer network information security is a challenge that must be faced. Aiming to address the challenges mentioned, the study focuses on using big data technology to optimize the protection capability of network information security (Chang & Seow, 2019). This research would improve the detection speed and accuracy of abnormal network information and expand the application direction of big data, consequently promoting intelligent protection of network security. At present, the study of network information protection technology in scientific research has been improving and can better address various dangerous network attacks and intrusion operations at this stage. However, with the emergence of big data technology, conventional anomaly network information detection technology is difficult to apply. Therefore, big data technology should be combined with traditional anomaly network information detection technology to develop a more efficient anomaly network information detection and protection technology (Zhu, 2021). However, in academic circles, the current research status of computer network information security and protection under the background of big data remains in the initial stage of development.

DOI: 10.4018/IJITSA.319722 *Corresponding Author

Since the rapid advancement of an information-based society, computer network information security has gradually become a popular research area. Several scholars have conducted scientific and comprehensive studies on this topic. Yang (2020) believed that computer network information security protection was the key direction for enterprises. He introduced computer network information security by analyzing and comparing numerous reference materials. Second, he analyzed the risks faced by computer network information security. Then, he noted that the computer network information security management system should be improved to strengthen security awareness and maintain the network security environment. His research summarized the application of protection strategies to maintain computer network information security, which provided a reference for related information security research (Yang, 2020). Deng (2020) pointed out that computer technology was increasingly used in work, life, and study. He analyzed the major problems of computer information systems in security protection. His study referred to network information security protection norms and guidelines and proposed multilevel and multifaceted protection technical measures for information security management systems. In addition, he investigated the design framework of a reliable information security management system, which provided a useful reference value for the design of the information security management system (Deng, 2020). Shi (2017) noted that network information security was dominated by a variety of factors, suggesting operation complexities during assessment. To address this challenge, he studied network information security assessment and used an assessment model and algorithm based on correlation clustering analysis. The relevant influencing factors were comprehensively analyzed, and the network security evaluation index system was developed. In addition, he calculated the category of network information security level by normalizing different evaluation indicators. His research proved the feasibility and operability of the evaluation model (Shi, 2017). Carapico and Farrand (2017) believed that protecting cyberspace had become one priority of cybersecurity policies. He believed that the field of network information protection included network crime, key information infrastructure, and network defense. He pointed out that the important role of the network detection department could be determined using the network supervision framework supplemented by network governance insights. In addition, he also guided the countermeasures of network information security supervision and proposed important decisions for protecting network information security (Carrapico & Farrand, 2017). The abovementioned research topics have also delved into computer network information security from multiple directions, and their findings played a guiding role in the growth of network information security; they also provided hints on the research content of this topic. Despite the increasing importance of computer network information security and big data, there remains a notable research gap in their relationship, indicating the urgent need for further exploration.

This research draws on various intelligent technologies used in global network information security protection studies, demonstrating that big data technology can be crucial in investigating network information security technology. Zou and Wu (2022) believed that the increase in the number of users and the acceleration of information and data flow not only provided convenience to everyday life but also provided opportunities for some unscrupulous elements to take advantage of, leading to the leakage of private information and data of enterprises and individuals. Therefore, strengthening network information security under big data is of great importance. This approach can effectively enhance network information security and improve the detection of abnormal network information (Zou & Wu, 2022). Fadhil et al. (2017) found that computer and communication network technology had been greatly improved in recent decades, which influenced the reform of big data technology. He argued that information security was related to the impact of big data applications on computer networks. Moreover, he pointed out that many external factors, which led to information leakage and resulted in huge economic losses, affected the security of information and big data on the network. Given these problems, he believed that improving awareness of protecting computer network information security had a proactive role in protecting computer and communication network security (Fadhil, Lubna, & Sayl, 2017). The studies of the abovementioned scholars have provided a

good direction for this work. However, their research also has some shortcomings. While the previous research was primarily theoretical, the conclusions lack specific practical applications. Building on this work, our present study aims to provide more practical test experiments to enhance the research finding applicability.

Currently, the promotion of network information technology is already in the phase of rapid promotion and optimization. However, the study on protecting network information security of computer systems has approached the bottleneck, which has always been the most concerned area of network detection departments. Therefore, this study optimizes and improves protection technology combined with the most developed big data technology. Compared with traditional network information detection and protection technologies, big data can speed up the analysis of abnormal network data. Furthermore, big data technology can also improve the efficiency of early warning response to network attacks, indicating a more intelligent network information security protection strategy.

## NETWORK INFORMATION SECURITY PROTECTION

### Importance of Network Information Security Protection

Currently, network attacks continuously beset the area of network information security, and network security incidents and accidents emerge endlessly. The impact of network information security varies over the individual, organizational, and social levels (Zhu, 2021; Niu et al., 2022). Worldwide, information virus attacks have repeatedly occurred in many countries, causing huge global economic losses. In addition, the harm of information security has spread to various industries, such as finance, energy, and medical care (Ye et al., 2020). Furthermore, Chinese users have suffered serious virus attacks, which have impacted their lives and work.

The information presented above indicates that the current network security environment is not optimistic and can no longer be ignored. Almost all information activities on the network are likely to be attacked and invaded, which has apparent effects on personal life, social stability, and national security. Among them, we can divide the focus of network information security protection into three aspects:

The reliability of network information security refers to the characteristics that the network system can complete information exchange under specific conditions to ensure information reliability. In network transmission and communication, the security and reliability of information is the primary goal. Therefore, as the basis of network security, the reliability of network information security is the most basic requirement of network system security.

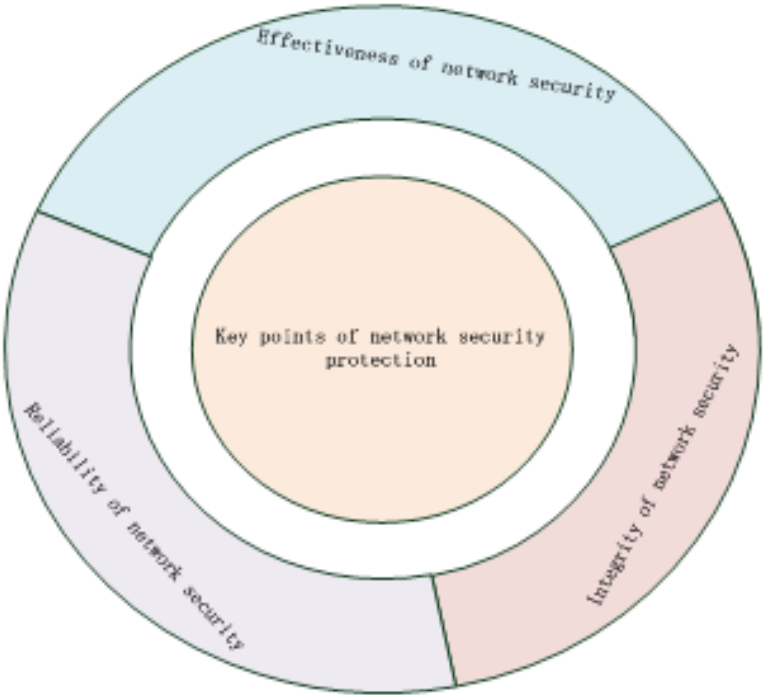
The effectiveness of network information security, while ensuring security and reliability, must also ensure the accuracy of data, which is the fundamental requirement of security applications. In any application and provision of Internet data, users can use the information correctly only when the data received or sent are valid; otherwise, such information is wrong.

The integrity of network information security, as the last feature of information security, refers to the notion that no one can change the data characteristics of the transmitted and collected information without authorization. Information is not modified, damaged, or lost during storage or transmission. Among them, the focus of network information security protection is shown in Figure 1.

### Features of Network Information Security

As the world is undergoing major changes and facing new crises and challenges in network technology and information security, the global community must strengthen solidarity and cooperation in the network world and safeguard fairness and justice to share data dividends (Ping, 2022; Ye, Shi, & Zhang, 2021). In securing security, the security technology platform should focus on consolidation to improve security protection. They should also conduct security publicity and popularization to strengthen international security cooperation. In addition, network information security has its characteristics, which can be divided into the following points:

**Figure 1.**
**Key Points of Network Information Security Protection**




1. **Vulnerability of network information security:** A network is a highly open network structure, and its vulnerabilities are caused by openness. However, openness itself also contains many defects. The higher the network's openness in the structure, the lower the security reliability. The vulnerability of the Internet is mainly reflected in its design, implementation, and protection. Although the risk of network security has been considered in the Internet design phase, it is insufficient in the design phase of security measures. Although various measures have been fully considered for network security design, the skills of Internet users, managers, and other competent elements easily restricted them in terms of the specific implementation process. In addition, in both the Internet design and maintenance stages, network keys and various environmental complexity factors easily interfered with security vulnerabilities, resulting in security problems. Therefore, objectively designed vulnerabilities and subjective operations are more harmful to the normal use of the network. They may threaten every network link at any time, resulting in network collapse, transmission omission, file infringement, and other serious consequences.
2. **Abruptness of network information security:** Most times, sudden damage from computer viruses is also an essential factor for security. Professionally, a computer virus is defined as an artificial code or command that can be quickly delivered and restored to state within a computer, with the fundamental characteristics of being destructive, spreading, and repetitive. The appearance of computer viruses is variable and often sudden, which damages important data in applications and operating systems, seriously endangering the normal use of computers and even stealing important data and information from computers. Concealment is also an important feature of computer viruses because it is a manual program. When viruses are transplanted into the computer, they do not immediately manifest destructiveness. Instead, they can coexist in the system for a period. The more time a virus remains hidden, the more information resources

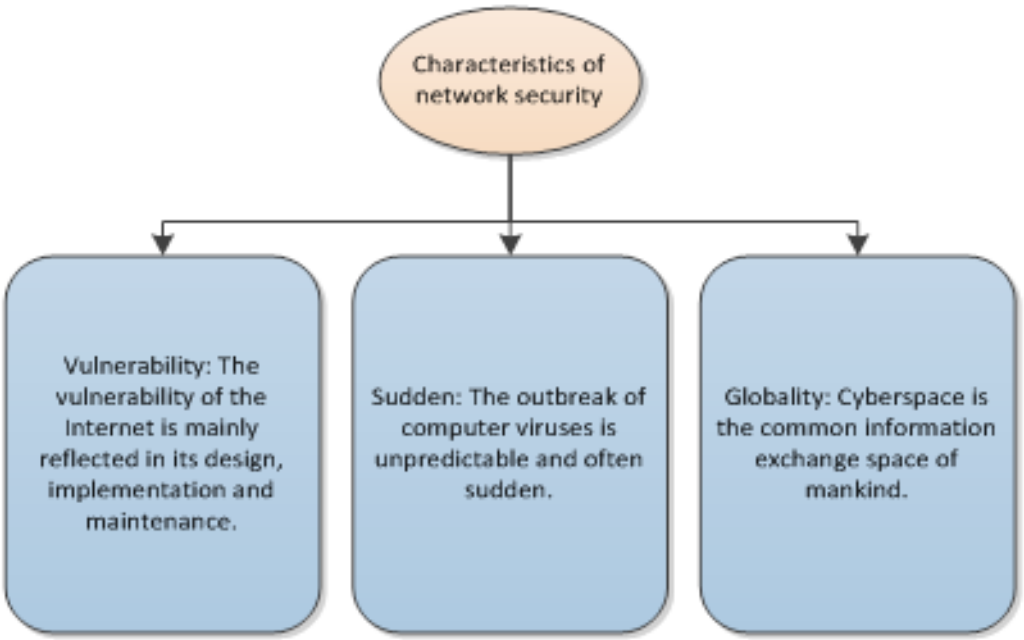
the virus gains. However, a virus outbreak causes widespread and rapid spread, quickly leading to many serious problems, such as information loss, information leakage, and network system paralysis. As a problem outside the traditional security field, the destructiveness of information is likely to occur undetected, which can quickly launch attacks without security response time. Information security departments and network security managers can address the sudden crisis of network information security by implementing preventive measures to minimize its harm.

3. **Globalization of network information security:** Cyberspace is the common information exchange space of mankind. Cyberspace is not controlled by one or more countries but should be jointly controlled by all countries worldwide. The rapid speed and wide range of Internet information dissemination have greatly facilitated human life. The interconnection of the Internet has greatly accelerated the process of global integration. However, with the exponential explosion of network information, many security problems have gradually emerged on networks. Relevant data show that widespread and substantial property loss caused by network security attacks has occurred worldwide. As a result, we must encourage international cooperation to ensure information security in cyberspace. All parties should adhere to multi-lateral and multi-party participation and respect network sovereignty. They should also focus on partnership and adhere to the spirit of cooperation, consequently aiding the promotion of international collaboration to deepen practical cooperation while jointly addressing risks and challenges. We present the characteristics of network information security in Figure 2.

## Network Information Security Attacks

At present, network information attacks emerge endlessly and seriously affect daily life. The information security of the Internet environment can be ensured by constantly reforming and improving information

**Figure 2.**
**Network Information Security Characteristics**



security technology (Jie, 2019; Vinitha & Suruthi, 2018). However, the law is stronger than the devil. Network information attack technology is also evolving, and various new technologies and vulnerabilities emerge endlessly. The following is a description of the main network attack technologies.

Internet attacks refer to illegal access or attempts to invade other computer systems. These attacks invade the Internet environment and invade clients or computer systems on the Internet. Network attack is a way for attackers to achieve the purpose of invasion. The degree of invasion changes from simply weakening the function of clients to destroying and limiting clients. The network attack mode generally follows three steps: detection, attack, and entry and exit. Initially, network attackers locate the target, collect information, and analyze the vulnerability of the target system. Then, the attacker uses computer and network technology to invade the other party's computer and its system through network weaknesses, and different damaging activities, such as gathering, modifying, destroying, and stealing information, are conducted.

The following are common network attacks:

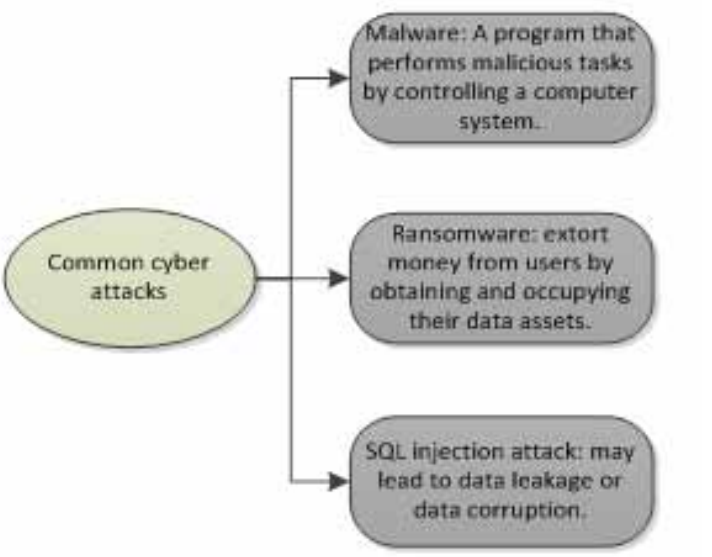
1. **Malware:** Malware is a procedure in which viruses, worms, and trojans perform malicious assignments on computer systems by controlling computer systems and destroying software processes. Malicious software is composed of various threat information, constantly emerging, and requires different methods and technologies to prevent viruses.
2. **Extortion software:** This software is a common virus software. It obtains and occupies users' data assets through harassment, intimidation, and even theft. The users' data assets include documents, e-mails, databases, images, and other important files. The user's data assets and computing resources cannot be used normally, and these important data and materials are used to threaten users and extort their money.
3. **Structured query language (SQL) code injection:** The mechanism of the SQL injection attack is to input data into the network application and use them for SQL query. The network application program does not strictly check the data entered by the user or may not even perform the required checking, which implies that users can splice and execute SQL commands. This limitation may lead to data leakage, corruption, lack of auditability, or even a complete takeover of the host. The five other types of injection technologies are Boolean blind injection, time blind injection, error-based injection, joint query injection, and heap query injection. We show the common network attacks in Figure 3.

## Anomaly Detection Concept of Network Information Security

Network anomaly detection aims to detect abnormal operations in systems or programs. As a result, abnormal behaviors of systems and programs quickly respond to improve the network's anti-attack ability and controllability and create a safe and stable network environment (Yu, 2021; Lin, 2021). Therefore, network anomaly detection is the basic technical support for maintaining network security and resisting network attacks and is an important guarantee for maintaining network construction and implementing business control. The research significance can be summarized as follows:

1. Network anomaly detection is the basic technical support needed to maintain network security and resist network attacks. At present, network infrastructure is facing various security threats brought about by network intrusion and penetration. The first step in fighting back is to find the intruder. The abnormal behavior of the quickly detected network can identify and prevent the intruder from the system before the intruder invades the network and endangers the system security, thus minimizing the system loss.
2. Network anomaly detection is an important guarantee for network construction and enterprise management. Through network threat detection, intrusion can be prevented to reduce the negative

**Figure 3.**
**Common Network Attack Behaviors**




impact on network availability, with weak links of the system identified, thus providing a basis for future decisions to strengthen network protection and network development. At the same time, network anomaly detection is an important part of network situational awareness. Through the normal anomaly detection model, they can quickly perceive abnormal events to further discover network system defects and vulnerabilities. As a result, targeted measures are taken in time to improve the stability of network service capabilities.

3. Network anomaly detection still has many problems and challenges in practical applications, such as low detection accuracy and poor availability. In multilevel network traffic information, traditional detection methods have difficulty detecting anomalies in the face of complex network information. Using various intelligent technologies, they can integrate this traffic information to enhance the detection capability of various network attacks and improve detection accuracy to reduce false positives and detection costs. This approach has a certain practical value for promoting the theoretical research and practical application of network anomaly detection.

## Anomaly Detection Technology for Network Information Security

We can consider network anomaly detection the last barrier against network information intrusion (Saidkulovich, Shoraimov, & Qudratov, 2021). Anomaly detection technologies are abundant, but only a few have become mainstream and are effective anomaly detection methods. We can briefly describe these approaches as follows:

1. Analysis of network anomaly detection technology based on machine learning (ML). Network anomaly detection technology based on ML has the special detection function of extracting information from network traffic and adaptively obtaining network traffic measurement values. As a result, various network environments can detect multiple network information attacks. ML technology continues to manifest great potential in detecting network anomalies alongside big data problems, which may play a role in anomaly detection in future big data network environments.

2. Network threat detection framework based on deep behavior analysis. At this stage, network intruders are constantly developing more threatening intrusion technologies. Better and more accurate intrusion strategies are used to perform network attacks, hence the difficulty of parrying traditional network information defense methods. Against the background of huge and complex network traffic, we regard this new network attack as a serious threat. Network intruders show violent attack behavior in network traffic, severely hindering traditional network information monitoring methods in unprecedented ways. Therefore, based on multilevel network detection technology based on integrated learning, a new network anomaly detection scheme based on deep behavior analysis is proposed, which meets the urgent requirements of network deep anomaly detection. Given the rapid development of big data analysis and cloud computing technology, we organically combined network protocol inverse analysis and network data flow processing technology to establish the basic theory and technical system of the network behavior mode.

## BIG DATA TECHNOLOGY AND NETWORK SECURITY

### Network Security Situational Awareness in the Big Data Environment

With the rapid advancement of big data, edge computing, and IoT technologies, networks are becoming increasingly closely combined with the social economy and daily life. As a result, the network structure has become more complex, and the data scale has become increasingly larger. However, with the increase in network security threats and security risks, network attacks are distributed and complex.

With the increasing threat of network attacks to network information systems, big data environments quickly identify network security risks and discover network security events, which can help predict the development trend of network security. Big data technology can also reduce network security risks and enhance security defense capabilities. Research on network security situational awareness technology in big data environments provides data acquisition and processing methods for network information monitoring, which has reference value for research on network security autonomous defense. Furthermore, identifying potential network security risks has been accelerated, providing a method reference for network security anomaly detection technology in big data environments.

Among them, the functions of big data security situational awareness technology are as follows:

1. **Big data:** Data drive is the basic attribute of the big data network security system and the maintenance concept of the system. The system relies on big data technology integration architecture, integrating information collection, storage, big data analysis, and situation awareness.
2. **Multidimensionality:** The network security situational awareness system can access multidimensional data sources, including various device logs, information data, behavior operations, etc. Second, the system includes monitoring, early warning, information transmission, and behavior tracking technologies. In addition, the technology can also collect the original data source and can quickly warn, notify, and respond to the threat information data input from outside.
3. **Intelligence:** The network security situation awareness system has an intelligent security analysis function, which enriches the internal data types. Business information, vulnerability scanning, attacker identification, and other relevant data are closely combined. We have adopted advanced big data statistics technology and data mining technology to further optimize the efficiency of querying and analyzing security data.

### Time Series Network Detection Algorithm Based on Big Data

The temporal network detection algorithm based on big data proposed in this research plays a prominent role in detecting and protecting computer network information intrusion. First, for the input network node $v_i$, its low-dimensional vector representation is obtained using the following linear transformation:

$$d_i = W_1 X_i + b_1 \tag{1}$$

where $X_i$ represents the attribute vector of node $v_i$, and $b_1$ is the offset vector.

In the information transmission structure of the network, information is transmitted through the neighbor of the metapath. For node $v_i$, the neighbor of metapath $l$ is $N_i^l$. The attention score of node $v_j$ is calculated as follows:

$$e_{ij} = \tanh\left(t_{ij} W^l d_j\right) + b^l \tag{2}$$

$$t_{ij} = \sum_{k \in K_{ij}^l} D\left(k\right) \tag{3}$$

Among them, $t_{ij}$ controls the time weight of node $v_i$ to node $v_j$. $K_{ij}^l$ indicates the combination of indexes in the network. In these networks, nodes $v_i$ and $v_j$ are connected to each other. The normalized exponential function is then used to normalize it. The calculation is expressed as:

$$\alpha_{ij} = \frac{\exp\left(e_{ij}\right)}{\sum_k \exp\left(e_{ik}\right)} \tag{4}$$

The attention score $\alpha_{ij}$ shows the effect of node $v_j$ on center node $v_i$. Therefore, to calculate the influence degree of all neighboring nodes on node $v_i$, the linear combination of node characteristics can be used to obtain the representation of $v_i$ nodes as follows:

$$d_{N_i^l} = \sum_{j \in N_i^l} \alpha_{ij} d_j \tag{5}$$

Then, node $v_i$ is fused through a linear rectification function to obtain the fused node function. The calculation method is given by:

$$d_i^{(1)} = RU\left(d_{N_i^l} + d_j\right) \tag{6}$$

The low-dimensional vector function $d_i^{(1)}$ of the node is obtained through information transmission. Then, the connection information between nodes is collected, and the output information is transmitted to the next information processing layer recursively. The calculation method is expressed as:

$$d_i = f\left(d_{N_i^l}, d_i\right) \tag{7}$$

Thus far, through multilayer propagation, the information of the temporal network can be collected through the multilayer network to obtain complex and changeable network information resources, which facilitates the analysis process of the characteristics of network information.

## COMPUTER NETWORK INFORMATION SECURITY AND PROTECTION EXPERIMENTS BASED ON THE BIG DATA ENVIRONMENT

### Testing of the Temporal Network Detection Algorithm Based on Big Data

After the proposed temporal network detection algorithm based on big data, it is not realistic to rely on theoretical studies only. Therefore, the detection effect of the algorithm must be determined in the actual test. In this experiment, the traditional anomaly network information detection technology and time-series network detection algorithm based on big data are tested under the same conditions by comparing the two experiments.

To ensure the same test conditions to the greatest extent, this test uses the same test hardware equipment to detect the same network information intrusion attack simultaneously. In addition, this experiment provides statistics on the following performance indicators. We describe the test outcomes in Table 1.

According to the test results in Table 1, the early warning rate, detection accuracy, and interception rate of the big data-based temporal network detection algorithm are 92.88%, 93.28%, and 94.12%, respectively, are higher than those of traditional abnormal network information detection technologies. In addition, the early warning time of the big data-based temporal network detection algorithm is 3541 ms, which is lower than that of traditional abnormal network information detection technology. Therefore, the comparative information presented above shows that the early warning rate, detection accuracy, and interception rate of the time-series network detection algorithm based on big data are superior. Moreover, its early warning time is lower, showing that the detection algorithm technology has a faster reaction. Therefore, from the earlier conclusions, the temporal network detection algorithm based on big data is superior to traditional abnormal network information detection technology.

### Computer Network Information Security and Protection Experiment

1. **Investigation direction:** Given the aim of this research, the investigation direction in this experiment is to test the security and protection degree of computer network information based on a big data environment. It is necessary to investigate the effectiveness of the time-series network detection algorithm using big data for protection in real-world network environments.
2. **Investigation content:** The survey entails two main aspects. First, the temporal network detection algorithm based on big data and the traditional abnormal network information detection technology are tested. The purpose is to investigate the change degree of this algorithm compared with traditional anomaly network information detection technology. Second, it investigates the protection and effect of big data temporal network detection algorithms on network information security.

**Table 1.**
**Performance Comparison of Different Anomaly Network Information Detection Technologies**

| | Traditional abnormal network information detection technology | Time series network detection algorithm based on big data |
|---|---|---|
| Early warning rate | 87.63% | 92.88% |
| Early warning time | 4552 ms | 3541 ms |
| Detection accuracy | 88.41% | 93.28% |
| Interception rate | 88.25% | 94.12% |

1. Early warning rate: This parameter shows the accuracy rate of identifying abnormal network information and warning operations.
2. Early warning time: This parameter indicates the early warning response time in collecting abnormal network information.
3. Detection accuracy: This parameter shows the accuracy of virus information detection when the device is attacked by virus information.
4. Interception rate: This parameter indicates the effective interception rate of harmful virus information, which is an important embodiment of network security protection technology.

3. **Investigation methods:** In this experimental survey, the control test and questionnaire survey are used. This scientific and logical experimental investigation method guarantees the scientific robustness and authenticity of the test experiment.
4. **Findings:** We conducted actual detection tests during the investigation of the big data-based temporal network detection algorithm and the traditional abnormal network information detection technology. In addition, we investigated the two algorithms to assess protection against various network attacks, including three performance evaluation indicators: the protection rate against malicious software, ransomware, and SQL code injection attacks. We present the final results in Figure 4.

Figure 4 shows that during the operation of the two network detection technologies, the protection rates of traditional anomaly network information detection technology and big data-based temporal network detection algorithm against malware are 87.25% and 93.85%, respectively, against ransomware are 88.33% and 92.86%, respectively, and against SQL code injection attacks are 86.75% and 92.55%, respectively. The comparative results indicate that big data's temporal network detection algorithm has a higher protection rate against various network attacks. This outcome proves that the temporal network detection algorithm based on big data is superior to traditional abnormal network information detection technology in protecting against network attacks.

In addition, the protective role and effect of time-series network detection algorithms based on big data on network information security must be investigated. Questionnaires were used to survey several network watchdogs. Similarly, the selected survey option is network information security's reliability, effectiveness, and integrity. We show the results of the questionnaire in Figure 5.

According to the questionnaire results in Figure 5, 68.31% of the network supervision organizations believe that the time-series network detection algorithm based on big data can greatly improve the reliability of network information security. Nearly one-third (68.73%) of the network supervision

**Figure 4.**
**Degree of Protection Provided by the Two Algorithms Against Network Attacks**

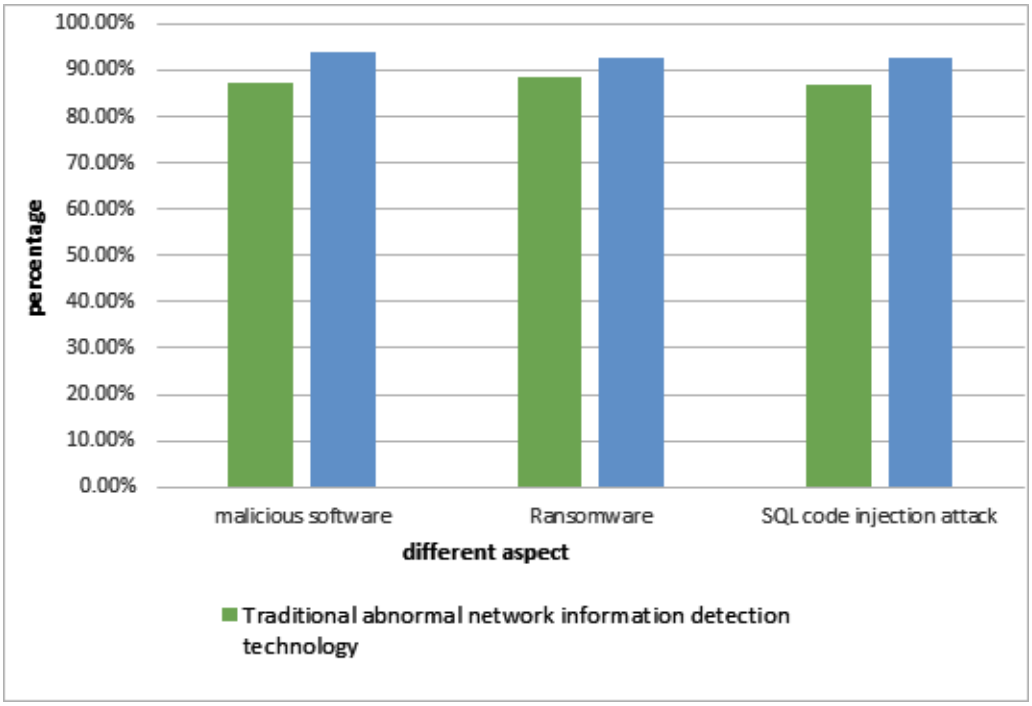
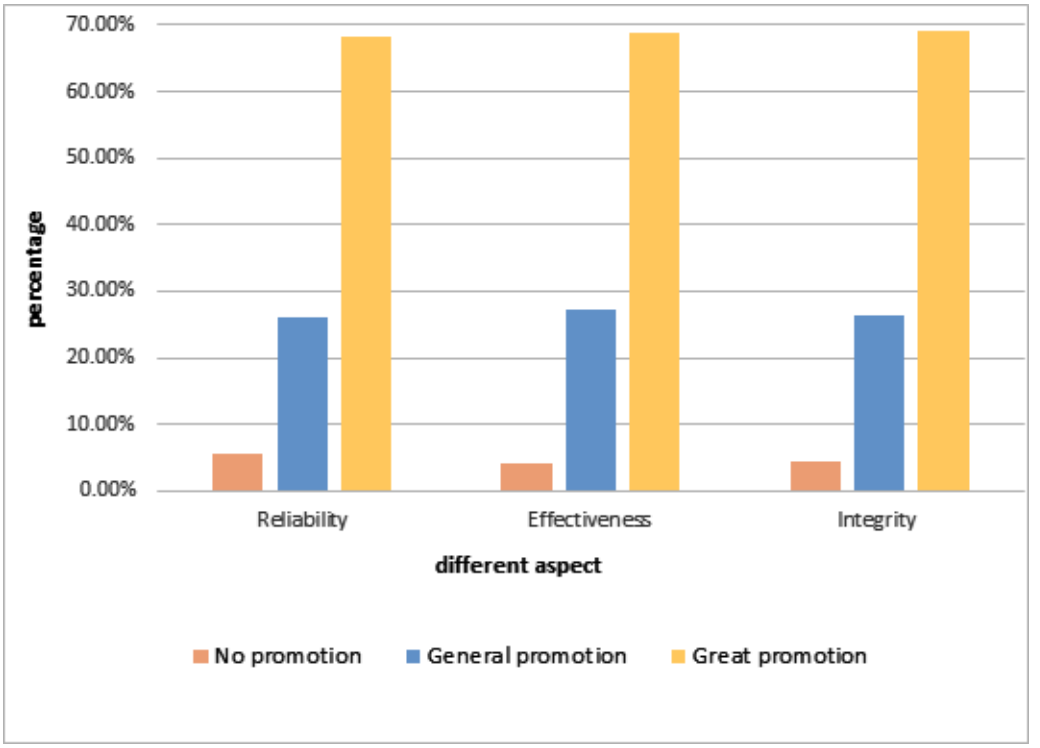


**Figure 5.**
**Survey of the Protection Effect of Network Information Security in the Big Data Environment**




institutions believe it has a greater role in improving the effectiveness of network information security. In addition, 69.12% of network supervision organizations believe that it greatly improves the integrity of network information security. The questionnaire results show that most network supervision organizations believe that after adopting time-series network detection technology based on big data, its protective role and effect on network information security have been significantly improved, which ensures the reliability, effectiveness, and integrity of network information security.

In summary, the experimental and survey results verify the enhanced protection against network attacks by the proposed algorithm, and it can improve all important aspects of network information security protection, suggesting this study's high value. This research not only attempts to improve the protection ability of network information security but also opens up the application potential of using big data in network information security detection technology.

## CONCLUSION

This study has proven the optimization of big data in network information security protection technology through rigorous theory and scientific testing methods. The test experiment results show that the temporal network detection algorithm based on big data can significantly improve protection against various network attacks and reduce the early warning time in collecting abnormal network information. Furthermore, this temporal network detection algorithm has fully improved the computing power of computing devices by connecting large databases and can more efficiently identify abnormal network information based on big data mining technology.

This research highlighted the importance of network information security and privacy and focused on performing computer network information security protection based on big data technology. As a result, a big data-centric network information security detection and governance framework was established. We expect the integration of network information protection and data security system development in this study to benefit future researchers. When the process of informatization is accelerating, its protection technology cannot fall behind. Overall, this research applied big data technology to network information security protection to further the protection effect, which guided the growth of network information security protection strategies through big data technology.

## REFERENCES

Carrapico, H., & Farrand, B. (2017). 'Dialogue, partnership and empowerment for network and information security': The changing role of the private sector from objects of regulation to regulation shapers. Crime, Law, and Social Change, 67(3), 245–263. doi:10.1007/s10611-016-9652-4 doi:10.1007/s10611-016-9652-4

Chang, K.-C., & Seow, Y. M. (2019). Protective measures and security policy non-compliance intention: IT vision conflict as a moderator. Journal of Organizational and End User Computing, 31(1), 1–21. doi:10.4018/JOEUC.2019010101 doi:10.4018/JOEUC.2019010101

Deng, Z. (2020). Computer network information security risks and solutions under the background of big data. Solid State Technology, 63(4), 7574–7582.

Fadhil, S. A., Lubna, E. K., & Sayl, G. A. (2021). Protection measurements of computer network information security for big data. Journal of Discrete Mathematical Sciences and Cryptography, 24(7), 1959–1965. doi:10.1080/09720529.2021.1959996 doi:10.1080/09720529.2021.1959996

Jie, H. (2019). A survey of network and information security. International Journal of Informatics and Computation, 1(2), 15–22. doi:10.35842/ijicom.v1i2.6 doi:10.35842/ijicom.v1i2.6

Lin, W., Yang, C., Zhang, Z., Xue, X., & Haga, R. (2021). A quantitative assessment method of network information security vulnerability detection risk based on the meta feature system of network security data. Transactions on Internet and Information Systems (Seoul), 15(12), 4531–4544. doi:10.3837/tiis.2021.12.015 doi:10.3837/tiis.2021.12.015

Niu, J., Alroobaea, R., Baqasah, A. M., & Kansal, L. (2022). Implementation of network information security monitoring system based on adaptive deep detection. Journal of Intelligent Systems, 31(1), 454–465. doi:10.1515/jisys-2022-0032 doi:10.1515/jisys-2022-0032

Ping, H. (2022). Network information security data protection based on data encryption technology. Wireless Personal Communications, 126(3), 2719–2729. doi:10.1007/s11277-022-09838-0 doi:10.1007/s11277-022-09838-0

Saidkulovich, M. S., Shoraimov, H. U., & Qudratov, S. A. O. (2021). The study on network information security. Galaxy International Interdisciplinary Research Journal, 9(6), 248–251.

Shi, K. (2017). Research on the network information security evaluation model and algorithm based on grey relational clustering analysis. Journal of Computational and Theoretical Nanoscience, 14(1), 69–73. doi:10.1166/jctn.2017.6126 doi:10.1166/jctn.2017.6126

Vinitha, K., & Suruthi, N. (2018). Enhancing the challenges of network information security using Industry 4.0 paradigm. International Journal of Engineering Research & Technology (Ahmedabad), 6(14), 1–5.

Yang, Y. (2020). Computer network information security and protection strategy. Frontiers in Economics and Management, 1(12), 1–5. doi:10.6981/FEM.202012_1(12).0001 doi:10.6981/FEM.202012_1(12).0001

Ye, C. Q., Shi, W. Y., & Zhang, R. (2021). Research on gray correlation analysis and situation prediction of network information security. EURASIP Journal on Information Security, 2021(3), 3. doi:10.1186/s13635-021-00118-1 doi:10.1186/s13635-021-00118-1

Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A risk analysis framework for social engineering attack based on user profiling. Journal of Organizational and End User Computing, 32(3), 37–49. doi:10.4018/JOEUC.2020070104 doi:10.4018/JOEUC.2020070104

Yu, G. X. (2021). Research on computer network information security based on improved machine learning. Journal of Intelligent & Fuzzy Systems, 40(4), 6889–6900. doi:10.3233/JIFS-189520 doi:10.3233/JIFS-189520

Zhu, X. (2021). Self-organized network management and computing of intelligent solutions to information security. Journal of Organizational and End User Computing, 33(6), 1–16. doi:10.4018/JOEUC.20211101.oa28 doi:10.4018/JOEUC.20211101.oa28

Zou, H., & Wu, Q. (2022). Optimization strategy of computer network information security from the perspective of cognitive impairment. Psychiatria Danubina, 34(suppl 1), 286–287.