Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 14, No. 2, 2024

New Challenges and Countermeasures of Network Security in the Context of Big Data

Zicong Lin *

Philippine Christian University Center for International Education, 1004, Manila City, Republic of the Philippines
* **Corresponding author Email:** 1651121576@qq.com

Abstract: With the wide application of big data technology, the problem of network security is becoming increasingly prominent. This study analyzes the new challenges of cybersecurity in the big data environment, including the diversity of data breaches, cyber-attacks, and the difficulty of privacy protection. At the same time, the limitations of traditional security measures in addressing these challenges are discussed, and a series of innovative coping strategies are proposed, including fine-grained access control technology, role-based access control, intelligent security detection, and the application of blockchain access control technology. By building a comprehensive security protection system, it aims to provide effective solutions for network security in the era of big data.

Keywords: Network security; Fine-grained access control technology; Role-based access control; Intelligent security detection; Blockchain access control technology.

1. Introduction

With the wide application of big data, the problem of network security has become increasingly prominent and has become the focus of attention from all walks of life. In the big data environment, the generation, storage and processing of data has shown an explosive growth trend. While enterprises and organizations use big data for analysis and decision-making, they also face multiple security threats such as data leakage, information tampering and cyber attacks. According to relevant statistics, in recent years, data leaks have occurred frequently around the world, bringing huge economic losses and credit crisis to enterprises and individuals. Traditional network security protection measures, such as firewalls and intrusion detection systems, mainly rely on static rules and feature matching, which is difficult to adapt to the complex and dynamic threats in the era of big data. Using big data analysis technology, cyber attackers can quickly identify vulnerabilities in the system and carry out precise attacks. This kind of attack not only increases the difficulty of security protection, but also makes the traditional security measures seem powerless. At the same time, in the big data environment, users' personal information is often widely collected and analyzed, leading to a significant increase in the risk of privacy disclosure. While pursuing commercial interests, many enterprises ignore the protection of user privacy, which leads to the illegal use or abuse of user data. This not only damages the legitimate rights and interests of users, but also makes enterprises face legal risks and reputation losses.

Therefore, in the face of network security challenges in the era of big data, it is urgent to build a new security technology system to cope with increasingly complex security threats. This article will explore the main challenges of network security in the big data environment, analyze the limitations of traditional security technologies, and propose a series of innovative coping strategies, including fine-grained access control technology, role-based access control, intelligent security detection, and the application of blockchain access control technology. By building a comprehensive security protection system, it aims to provide effective solutions for network security in the era of big data, so as to protect the legitimate rights and interests of enterprises and users, and promote the healthy development of big data technology.

2. Network security risks in the big data environment

2.1. Risk of data breach

A data breach is when sensitive information is obtained, used, or disclosed by an unauthorized person or organization. Data breaches can occur for a variety of reasons, including cyber attacks, insider mistakes, and system vulnerabilities. Cyber attackers try to gain access to sensitive information through various means, such as phishing attacks, malware, and social engineering. GoUpSec in-depth statistical analysis of data breaches around the world in 2023, in which government departments, technology companies, digital product manufacturers, automobile manufacturers, schools, mobile phone manufacturers, medical institutions, web portals, banking, airlines and other ten industries have become the most affected by data breaches. There were several major data breaches in 2023. For example, T-Mobile's data breach involving 37 million accounts is expected to incur significant investigative costs. The source code repository of Russian tech company Yandex was stolen by a former employee and publicly posted on a hacking forum, leaking 44.7 GB of files. Blockchain wallet BitKeep has suffered a cyber attack, with attackers stealing more than $9 million worth of digital currency through a malicious Android app.

2.2. The complexity of the means of cyber attack

In the big data environment, the means of cyber attack are increasingly complex and diverse. Cross-site scripting (XSS), for example, is a common form of cyber attack, accounting for about 40% of all cyber attacks. Despite its prevalence, most cross-site scripting attacks are not sophisticated and are usually launched by junior cybercriminals using off-the-shelf scripts. Cross-site scripting attacks target website users, not the Web application itself. By injecting malicious code on a

vulnerable website, attackers trick website visitors into executing that code. This malicious code can be used to steal user account information, install trojans, and even tamper with website content to mislead users into revealing personal privacy. A distributed denial of service (DDoS) attack does not directly breach a website's security, but it can make it temporarily or permanently inaccessible. According to Kaspersky Lab's 2017 IT Security Risk Survey, the average cost of a single DDoS attack to a small business is around $123,000, while large enterprises can lose up to $2.3 million. DDoS attacks flood the target Web server with a large number of requests, thus making the website inaccessible to other users. Attackers typically make use of botnets, which are made up of previously infected computers capable of coordinating a large number of requests from around the globe. In addition, DDoS attacks are often used in combination with other means of attack, and attackers may use DDoS to distract the attention of the security system, and then exploit the system vulnerabilities for further intrusion. In the Open Web Application Security Project's (OWASP) latest Top 10 application Security Risks report, injection vulnerabilities are listed as the most serious security threat. Among them, SQL injection is the most common injection attack mode. The primary targets of injection attacks are websites and their back-end databases. Attackers gain access to hidden data and user input by inserting malicious code to gain permission to modify data or even take full control of the application. This type of attack can directly affect the database security of websites and servers. In addition, another common cyberattack technique is to hide malicious program code and mask it. Cyber attackers often exploit existing security vulnerabilities, resulting in a variety of security and privacy breaches. This shows that the diversity of network security attack forms poses a significant threat to the secure and stable operation of the network, and may even lead to the complete collapse of the entire network system.r

2.3. The challenge of privacy protection

With the advancement of data collection and analysis technology, users' personal information is widely collected and exploited without their knowledge, resulting in a significant increase in the risk of privacy disclosure. While pursuing commercial interests, many enterprises often ignore the protection of user privacy, resulting in illegal acquisition and abuse of user data. The challenges of privacy protection are mainly reflected in several aspects. First, the centralized storage of data makes users' sensitive information more vulnerable to attack. Once the data is leaked, the user's personal information may be used for identity theft, financial fraud and other criminal activities, which brings serious security risks to users. Second, many companies lack transparency in their data processing, making it difficult for users to understand how their data is being used and shared. This kind of information asymmetry makes the user's trust in the enterprise decrease, and then affects the enterprise's reputation and market competitiveness.

3. Limitations of traditional network security technologies

3.1. Insufficient static protection mechanism

Traditional network security technologies mainly rely on static rules and feature matching, and often show slow response and high false positive rate in the face of dynamic threats in the era of big data. In static protection mechanism, firewall and intrusion detection system are usually based on known attack patterns and rules, and cannot effectively deal with new and complex attack means. As cyber attack techniques continue to evolve, attackers are often able to quickly find ways to bypass these protection mechanisms. Attackers of traditional firewalls can evade detection by encrypting traffic or using covert communication channels to achieve attacks on target systems. Therefore, static protection measures alone can not meet the needs of modern network security.

3.2. Lack of comprehensive and coordinated protection capabilities

Traditional network security technologies are often isolated and lack comprehensive and collaborative protection capabilities. Different security devices and technologies often do not work together effectively, leading to blind spots and vulnerabilities in security protection. For example, firewalls may not be able to share information with intrusion detection systems, missing potential security threats. The lack of a holistic perspective of the security protection system, so that enterprises in the face of complex network attacks, unable to form an effective force, reducing the overall security protection effect.

3.3. It does not adapt to the rapidly changing network environment

With the rapid development of cloud computing, Internet of Things and mobile Internet, the network environment has become more complex and dynamic. Traditional network security technologies are often difficult to adapt to this rapidly changing environment and cannot effectively protect emerging network architectures and application scenarios. The multi-tenant architecture and dynamic resource allocation in cloud computing environments make traditional security measures difficult to implement. In addition, the widespread application of iot devices has also brought new security challenges, and traditional technologies are difficult to cover the security needs of these devices.

4. Limitations of traditional network security technologies

4.1. Fine-grained access control technology

Data access control is an important link to ensure data security, especially in the big data environment, fine-grained access control is particularly important. By establishing a strict access control mechanism, you can effectively prevent unauthorized users from accessing and manipulating sensitive data. Fine-grained access control technology By establishing a ternary model of subject, object and operation, the user can achieve fine-grained access control in different terminals, databases and application systems. Compared with traditional coarse-grained access control methods, fine-grained access control provides more detailed and dynamic permission management. This technology enables system administrators to set and adjust access rights based on a variety of conditions, such as the identity of the user, the role, the requested action, the type and sensitivity of the data, so as to achieve a finer protection of data and resources. In practice, fine-grained access control is widely used in database systems, enterprise applications, and cloud computing environments. In database administration, fine-grained access control allows

administrators to precisely configure access to database tables, rows, columns, or views. This improves data security by preventing unauthorized users from accessing or modifying sensitive data. In enterprise applications, the technology enables the dynamic adjustment of permissions based on the specific needs of users and business rules to meet complex business scenarios and compliance requirements. In a cloud computing environment, fine-grained access control technology can dynamically adjust a user's access to data based on their identity, role, and authority, ensuring that only authorized users can access sensitive information.

4.2. Role-based access control

Role-Based Access Control (RBAC) is a common access control model that simplifies permission management by associating users with roles. The main advantage of RBAC is its flexibility in expressing and enforcing an organization's security policies, allowing administrators to operate according to day-to-day organizational management rules without having to dive into the underlying implementation. RBAC is seen as a more widely applicable access control model that can effectively formulate and enforce security policies for specific transactions, while alleviating bottlenecks in traditional security management. The RBAC model can be implemented at multiple levels. At the operating system level, such as Windows NT and Windows 2000, RBAC is used for user, user group, and permission management, but its security is limited by the characteristics of the operating system. Database systems such as Oracle and Microsoft SQL Server also support RBAC, and role management is included in the SQL 3 standard, but this implementation is also limited by system capabilities. Application-level implementations provide greater flexibility in application and Web environments, where RBAC manages permissions by controlling URL access and invoking apis. In a big data environment, RBAC can be combined with fine-grained access control for more flexible rights management. By defining the rights of different roles, enterprises can quickly adjust user access rights to meet changing service requirements.

4.3. Implement intelligent safety testing

4.3.1. Machine learning-driven intrusion detection system

Unlike traditional intrusion detection systems (IDS), machine learning-powered systems not only recognize known attack patterns, but also respond to novel attacks and unknown threats. This is because machine learning methods are capable of dynamically analyzing network traffic and user behavior to detect patterns of unusual activity and potential attacks. Through automatic learning and adaptation, this method can maintain high detection accuracy in the face of ever-changing attack means. In cyberspace security research, the application process of machine learning usually includes the following key steps: Firstly, the network security problem is abstracted to clarify the specific problems and goals that need to be solved; Then, data collection is carried out to collect relevant network traffic and user behavior data. The data is then preprocessed and security features extracted in order to convert the data into a format suitable for model training. In the model building phase, the detection model is constructed by selecting and training appropriate machine learning algorithms. After that, the model validation phase evaluates the model's performance on real data to ensure its validity and accuracy. Finally, the actual application effect of the model is tested through effect evaluation, and it is adjusted and optimized according to needs to improve its performance in the actual environment. Through this process, researchers can continuously optimize intrusion detection systems and improve their detection capabilities against new and unknown attacks, thus enhancing the level of network security protection.

4.3.2. Behavior analysis and anomaly detection

The behavior analysis technology collects the user behavior data in real time, uses the appropriate time sliding window for analysis, and inputs the data into the data analysis model. After the model analysis, the judgment of whether the user's behavior is normal will be provided to help the user make subsequent decisions. Anomaly detection models normal behavior in the system and treats behavior not covered by the model as an exception. Three matching methods can be selected to identify abnormal behavior: threshold method, by detecting the number of unmatched system calls to judge the anomaly; Mismatch rate, using the Hamming distance between sequences to determine the mismatch ratio to identify anomalies; Hamming distance, which measures the minimum Hamming distance between sequences to distinguish between abnormal and normal behavior, although this method is simple, it is less efficient when dealing with complex programs. The early behavior analysis method based on system call sequence explored the use of basic program abstraction and low-cost dynamic analysis to improve the accuracy of anomaly detection, and became a successful anomaly detection technology, which led to related research and the proposal of similar schemes. Therefore, behavior analysis and anomaly detection build a normal behavior model by monitoring the behavior of users and devices in order to detect abnormal activities in time. For example, in an enterprise network, if a user accesses a large amount of sensitive data in a short period of time, or performs abnormal operations during non-working hours, the system can automatically trigger an alarm and take corresponding measures. This intelligent anomaly detection can effectively reduce the risk of data leakage and network attacks.

4.4. Blockchain access control technology

Blockchain has a distributed structure, transparent transaction records, and is difficult to tamper with, while its trusted mechanism does not rely on third-party endorsements. In the context of big data, blockchain access control technology has been favored and applied in many fields because of its high credibility and difficult to tamper with. Blockchain 1.0 is mainly applied to virtual currency systems and involves functions related to cryptocurrencies such as payments, transfers, and auditing. Blockchain 2.0 focuses on smart contracts, aiming to take advantage of the high degree of trustworthiness of blockchain and use it as a programmable distributed trust infrastructure to expand applications to authentication, auctions, intellectual property protection and other areas where trust mechanisms need to be established. Although the specific definition of blockchain 3.0 is not clear, its core idea is to build an actual distributed system on the basis of blockchain 2.0, and further expand the application scope to the fields of government, industry, medical and art, to achieve a wider range of trusted "asset" transactions. Blockchain is a specific data structure formed by a chain of data blocks in chronological order in a peer-to-peer network environment. The architecture is composed of multiple core

layers, such as P2P network technology, cryptography technology, consensus mechanism, smart contract, etc. All nodes participate in data maintenance, even if a single node is tampered with or destroyed. There is no damage to the data stored in the block. The data layer is responsible for storing the core data of the blockchain and ensuring the integrity and immutability of the data through the hash function; The network layer realizes the information transmission and transaction verification between nodes through P2P network. The consensus layer ensures network consistency through consensus mechanisms such as PoW and PoS. The contract layer executes smart contracts and ensures automated operation with virtual machines; The application layer covers decentralized applications (DApps) and wallets, etc., to promote the application of various scenarios; The incentive layer encourages nodes to participate in network maintenance through token mechanism. All levels work together to ensure the security, transparency and decentralization of the blockchain.

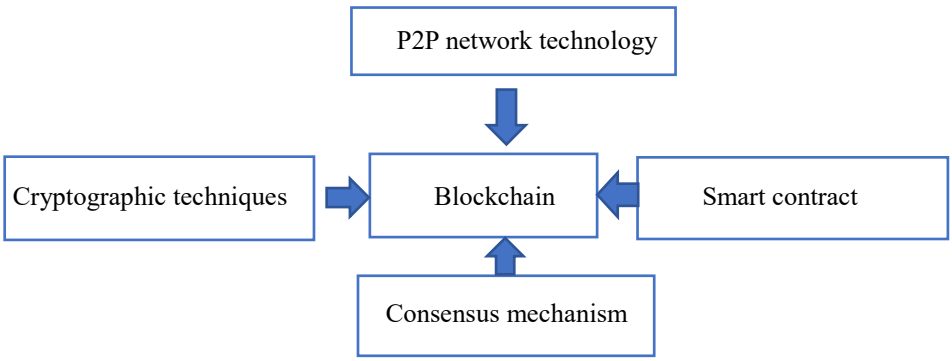

Figure 1. Blockchain core composition

4.5. Simplify the authentication mechanism

4.5.1. Multi-factor authentication

Multi-factor authentication (MFA) is an effective security measure that adds additional authentication steps, such as SMS verification codes and biometrics, on top of the traditional user name and password authentication. After MFA is enabled, users not only need to enter a user name and password when logging in (preliminary authentication), but also need to perform additional authentication through another method. Through this multi-level authentication mechanism, MFA is able to provide stronger security protection for accounts and resources. Using MFA authentication to confirm the authenticity of the user, even if the attacker obtains the user's password, he cannot easily pass the authentication, thus improving the security of the account.

4.5.2. Biometric identification technology

Biometric recognition technology includes but is not limited to face recognition, fingerprint recognition, iris recognition, etc. Face recognition technology captures facial images, identifies and records facial feature points through feature extraction algorithms, such as the position of the eyes, nose and mouth, and generates unique facial feature vectors. These feature vectors are then compared with known facial features stored in the database to identify the individual and perform authentication. Fingerprint recognition is one of the earliest biometric identification technologies, which is widely used in many fields. A fingerprint consists of the ridges of the fingertips, where the protruding part is called the ridge, and the part between the ridges is called the valley. These lines are often discontinuous, with frequent breakpoints, forks and turns, and these features are called minutiae, which provide unique identifying information for the fingerprint. Fingerprint recognition mainly includes three steps: feature extraction, fingerprint classification and matching decision. Feature extraction involves obtaining details from fingerprint images, such as direction field estimation of ridge line, ridge line extraction and detail extraction. Fingerprint classification speeds up the recognition process by identifying the direction of feature points and ridges. The matching decision stage determines whether two fingerprints are from the same finger, including string based matching, Hough transform matching and 2D dynamic regularization matching. Located between the pupil and the sclera, the iris is a highly unique and stable biological feature. The texture structure of the iris is formed during embryonic development and remains unchanged in adulthood, which is less affected by environmental factors and has good anti-counterfeiting. The iris recognition system is not in contact with the human body, is easy to use, and its annular nature makes analysis simple. The recognition process includes: iris localization, that is, segmenting the iris from the image and accurately locating its inner and outer boundaries; Iris alignment, through polar coordinate system or image registration technology to ensure the accurate correspondence of feature structure; Pattern expression, using multi-scale analysis and Gabor wavelet or Laplacian Gaussian filter to encode iris features; Matching decision, by calculating Hamming distance or correlation to judge the matching degree of two iris images. Based on the user's physiological characteristics, these biometric identification technologies are unique and difficult to forge, and can effectively prevent unauthorized access. In a big data environment, a higher level of security can be achieved in combination with the authentication mechanism of biometric identification technology.

5. Literature References

In the era of big data, technological advances have brought serious challenges to privacy disclosure. Dong (2023) analyzed the impact of big data on the right to privacy, discussed the dilemma faced by the privacy protection mechanism in China, and proposed to solve the privacy protection problem by improving the relief mechanism, enhancing civic awareness and strengthening data supervision. [1] Niu (2023) discussed data security issues in the era of big data, emphasizing the security risks brought by the scale and complexity of data. This paper analyzes the potential threats to network data security, and suggests that these challenges should be addressed by improving the early warning system, raising users' awareness of protection and

establishing a data protection system. [2] Xu (2024) discussed the challenges faced by computer network security in the big data environment and their countermeasures. The paper analyzes the limitations of traditional technologies in dealing with data breaches, cyber-attacks and illegal use of private data, and proposes to build a new security technology system, including blockchain, machine learning and biometrics, to enhance risk prevention and intelligent response. [3] Zou (2006) introduced the basic features and models of role-based access control (RBAC), including RBAC96 and ARBAC97. The paper explores how RBAC simplifies rights management by adding a role layer between users and permissions, and points out its broad applicability compared to traditional DAC and MAC technologies. [4] Gao, Cao et al. (2021) summarized blockchain-based access control technology and analyzed two implementation methods based on transactions and smart contracts and their advantages. The paper explores key technologies for dynamic access control, on-chain space optimization, and privacy protection, and presents challenges and prospects for future research, pointing out the potential of blockchain in decentralized access control. [5] Liu Ao et al. (2019) proposed a blockchain-based access control mechanism, BBAC-BD, which combines the ABAC model and blockchain technology. This paper describes the architecture, access control process and smart contract application of this mechanism, emphasizes its advantages of transparency, security and automated management in big data environment, and verifies its effectiveness through experiments. [6] Sun and Qiu(2001) reviewed the basic principles, key technologies, advantages and disadvantages of biometric identification technology, and discussed the existing problems and future research directions. The paper points out that this technology is based on the unique physiological and behavioral characteristics of individuals, and has wide application prospects, and ADAPTS to the increasing security needs. [7] Lin and Feng (2007) reviewed the traditional strategies of access control technology (DAC, MAC, RBAC) and their applications, introduced the UCON model, and discussed the research status and development trend in grid, P2P, and wireless networks. This paper emphasizes the necessity of trusted network and its impact on access control model, and points out that future research will focus on distributed system, flexible security policy and integrated security technology of trusted network. [8] Feng and Li et al. (2022) discussed the risks and challenges of information security in the big data environment and proposed corresponding risk prevention and control strategies. The paper emphasizes the importance of improving the efficiency of data use while ensuring information security, and points out that the accuracy and effectiveness of geological disaster monitoring and early warning can be improved in order to reduce the harm caused by disasters.[9] Zhao (2022) analyzed the security problems of computer networks in the context of big data, including hacker attacks, virus spread, etc., and proposed targeted prevention strategies, such as account protection, improving protection technology and strengthening network monitoring. The importance of refining prevention strategies and strengthening monitoring to ensure network security is emphasized.[10] Zhang et al. (2017) reviewed the application of machine learning in cyberspace security, and discussed the research progress and challenges in the fields of malicious web page identification and device identity authentication.[11] Zhou, Cui et al (2009) analyzed the behavior analysis technology in intrusion detection systems, and discussed the static and dynamic analysis methods of HIDS and their development trends and challenges.[12]

6. Conclusion

This paper explores new challenges to cybersecurity in the big data environment, including data breaches, the diversity of cyber-attacks, and the difficulty of privacy protection, and points out the limitations of traditional security measures. To address these challenges, innovative strategies such as fine-grained access control, role-based access control, intelligent security detection and blockchain technology are proposed, aiming to build a comprehensive security protection system, protect the rights and interests of enterprises and users, and promote the healthy development of big data technology.

Acknowledgment

In the process of writing this paper, I would like to sincerely thank all the people who have silently supported and encouraged me.

First of all, I want to thank my family. They have always supported me in pursuing my dream of academic knowledge, both spiritually and materially, and their support is the source of motivation for me to keep moving forward.

Secondly, I want to thank my friends. When I need to relax and divert my attention, their company and understanding make the whole writing process more enjoyable and relaxing.

In addition, I would like to thank those classmates and colleagues who have provided advice and help in their academic studies. Their discussions and sharing provided me with new ideas and insights.

Finally, I would like to thank all the people who have provided help and support for this paper. Although I cannot list them all, your contributions and help mean a lot to me. Your support and encouragement made it possible for me to finish this paper. Once again, I would like to express my sincere thanks to you.

References

[1] Dong , Privacy Protection Dilemma and Relief in the Era of Big Data, Legal Review, No. 15, 2023, P46-47.

[2] Niu, Analysis and Discussion of Data Security under Big Data Environment, Electronic Communication and Computer Science, 2023, Vol. 5, No. 3,P149.

[3] Xu , Optimization Strategy of computer network security technology in the era of big Data, Electronic Components and Information Technology,2024.3.049, P194-195.

[4] Zou, Role-Based Access Control Model Analysis and Implementation, Microcomputer Information, Vol 22, No. 6-3, 2006, P108-110.

[5] Gao , Cao , et al, Research Progress of Blockchain-based Access Control Technology, Journal of Network and Information Security, December 2021, Volume 7, Issue 6 P69-72.

[6] Liu , Du et al., Blockchain-based Big Data Access Control Mechanism, Journal of Software, 2019,30 (9),P2639.

[7] Sun , Qiu , Review of Biometric identification technology, Journal of Electronic Sciences, No. 12A, December 2001, P1745.

[8] Lin , Feng , Access Control Technology in new network environment, Journal of Software, Vol.18, No.4, April 2007,P959-961.

[9] Feng , Li et al., 2022, Inner Mongolia Science and Technology and Economy, No. 10, May 2022, P92-93.

[10] Zhao , Analysis of Computer Network Information Security in the context of Big Data, No. 6, 2022, P108-109.

[11] Zhang, cui , etc., machine learning in the study of cyberspace security research, computer journal, 2017, p3-4.

[12] Zhou , Cui , et al. Anomaly Detection technology based on System Behavior Analysis, Telecommunications Science, 2009 (2), P60-62.