Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 4, No. 3, 2023

Research on Computer Network Security Prevention in the Context of Big Data

Jiahao He *

Chongqing Jiaotong University, Chongqing, China
*** Corresponding author Email:** biankakiahoo@gmail.com

Abstract: With the rapid development of information technology, big data technology has become one of the important pillars of today's society. However, the wide application of big data has also brought more security threats and challenges, among which computer network security has become a focus that needs to be solved urgently. This thesis aims to study the current situation and challenges of computer network security in the context of big data, analyze the advantages and disadvantages of the existing security measures, and put forward improvement programs to better protect computer network security in the era of big data.

Keywords: Big Data; Cyber Security; Importance.

1. Introduction

With the rapid development of information technology and the arrival of the big data era, computer network security issues are becoming increasingly prominent. Network attacks are constantly upgrading, and traditional security defense means have been difficult to cope with the increasingly complex and changeable threats. In such a context, the construction of a more efficient and intelligent network security defense system has become an urgent problem to be solved. This dissertation aims to explore the research related to computer network security prevention in the context of big data, with a special focus on the application of big data analytics technology in network security, as well as the intelligent security monitoring and response system based on artificial intelligence, and also on encryption algorithms for enhanced data privacy protection. This thesis aims to provide a comprehensive and in-depth perspective on the new trends and methods of computer network security prevention in the context of big data. Through the comprehensive use of big data analysis technology, artificial intelligence algorithms and encryption algorithms for enhanced data privacy protection, we can establish a more powerful and intelligent network security defense system to provide strong support for the robust development of network security. In the future research and practice of network security, the content provided in this paper will have a positive impact on the innovation and development of network security technology.

2. The Application of Big Data Analysis in Network Security

2.1. Application of Big Data Analytics in Intrusion Detection

Intrusion Detection System (IDS) is an important part of computer network security, used to monitor and identify abnormal behavior and potential attacks in the network. In the context of big data, traditional IDSs may face the challenge of dealing with massive data and highly complex network environments. Therefore, the enhancement and optimization of intrusion detection using big data analytics has become an important research direction.

2.1.1. Log Analysis

In the big data environment, the amount of log data generated by network devices and systems is huge, and traditional IDS is often difficult to process and analyze this data effectively. By applying big data analysis technology, large-scale log data can be analyzed in real time or offline, from which abnormal patterns and abnormal behaviors can be extracted, helping to quickly discover potential intrusion threats.

2.1.2. Behavioral Analysis

Big data analytics can build models based on user and device behavioral data and identify abnormal behaviors that do not conform to normal behavioral patterns. Through in-depth analysis of network traffic, application usage, and user behavior, intrusions can be more accurately detected, including attacks with unknown, zero-day vulnerabilities.

2.1.3. Threat Intelligence Analysis

Big data analysis can integrate threat intelligence data from different sources, including hacker forums, vulnerability information, malware samples, etc., to form a comprehensive threat intelligence database. By correlating and analyzing with real-time network traffic and event data, potential threats can be detected earlier and the detection accuracy and real-time performance of IDS can be improved.

2.1.4. Data Mining Technology

In the big data environment, traditional rule and signature-based intrusion detection methods may not be able to cover all intrusion scenarios. Data mining technology can mine potential patterns and association rules in massive data to help discover new types of attacks and anomalous behaviors, thus improving the coverage and accuracy of intrusion detection.

2.1.5. Machine Learning Algorithms

Machine learning plays an important role in big data analytics and is particularly applicable to intrusion detection. With training datasets, machine learning algorithms can learn the normal behavioral patterns of the network and automatically identify abnormal and malicious behaviors. Over time, machine learning models can also adaptively adjust to changing means of intrusion.

2.1.6. Distributed Computing

Big data analytics typically involves distributed computing

techniques to handle massive amounts of network data. By distributing intrusion detection tasks to multiple nodes for parallel processing, detection speed can be accelerated and system scalability can be improved.

In summary, the application of big data analytics in intrusion detection can enhance the detection capability of IDS and improve the accuracy and real-time nature of intrusion detection. Through the comprehensive application of log analysis, behavioral analysis, threat intelligence analysis, data mining technology, machine learning algorithms and distributed computing, the abnormal and invasive behavior in the network can be better discovered, so that corresponding defensive measures can be taken early to protect the security of the computer network.

2.2. Application of Big Data Analysis in Behavior Analysis

Behavioral analysis is a method of identifying potential threats based on their behavioral patterns through real-time monitoring and analysis of the behavior of network users and devices. In the context of big data, traditional behavioral analysis methods may not be efficient and accurate enough due to the excessive amount of data and complex network environment. Therefore, the use of big data analytics in behavioral analysis has become an important way to improve and optimize behavioral analysis.

2.2.1. User Behavior Analysis

Big data analytics can monitor and analyze user behavior on the network in a comprehensive and detailed way. By collecting and analyzing data such as users' access patterns, clicking behaviors, and operating habits, a user's behavior model can be established. Once abnormal user behavior is found, such as abnormal login locations, frequent access attempts, etc., the system can immediately take measures for risk alert or blocking.

2.2.2. Application Behavior Analysis

Big data analytics can monitor and analyze application behavior and identify potential abnormal activities. By analyzing application operations and resource usage, possible vulnerability exploits, malicious code injections, and abnormal application behaviors can be identified. This helps to identify application vulnerabilities early and take remedial action.

2.2.3. Device Behavior Analysis

For devices in large-scale complex network environments, such as IoT devices and industrial control systems, big data analytics can monitor the behavior of devices in real time. By establishing the behavioral model of the device, abnormal behavior of the device, such as the device being infected, attacked or subjected to unauthorized access, can be detected in time, thus preventing potential security threats.

2.2.4. Threat Intelligence Fusion

Big data analysis can fuse and analyze data from multiple threat intelligence sources to form a comprehensive threat intelligence database. Combining threat intelligence with real-time behavioral analysis can more accurately identify potential threats, including zero-day attacks, advanced persistent threats, and so on.

2.2.5. Anomaly Detection

Using big data analysis technology, it is possible to establish a normal behavior model for network behavior data, and then detect the difference between the actual behavior and the model in real time. Once abnormal behavior is detected, the system can respond by means of alarms or blocking to protect the security of the network.

2.2.6. Data Visualization

The application of big data analytics in behavioral analysis also includes data visualization. By converting complex behavioral data into visual charts and images, the anomalies and trends in the network can be displayed more intuitively, helping security personnel better understand the network security situation and make quick decisions.

2.3. Application of Big Data Analytics in Threat Intelligence

Threat intelligence is the process of collecting, analyzing and interpreting information related to network security to identify potential threatening behaviors and attack activities. In the context of big data, network security threats are increasing, and traditional methods of collecting and analyzing threat intelligence can no longer meet the complex and changing threat situation. Therefore, the application of big data analysis technology in threat intelligence becomes particularly important to improve the accuracy, real-time and comprehensiveness of threat intelligence.

2.3.1. Threat Intelligence Collection and Integration

Using big data analytics, a large amount of threat information can be collected from multiple threat intelligence sources, including hacker forums, vulnerability databases, malware sample libraries and so on. Then, through data integration and generalization, the threat intelligence from different sources is fused to form a comprehensive threat intelligence database, which provides basic data for subsequent analysis.

2.3.2. Threat Intelligence Analysis

Big data analysis technology can analyze threat intelligence in depth, from which hidden patterns, trends and association rules can be found. Through mining and correlation analysis of threat intelligence data, potential threat behaviors can be more accurately identified, including new types of threats, zero-day vulnerability exploitation and advanced persistent threats.

2.3.3. Real-time Threat Intelligence Monitoring

Big data analytics can monitor and analyze real-time network traffic and event data to discover and respond to emerging threats in a timely manner. By correlating with the threat intelligence database, behaviors related to known threats can be quickly identified and timely defensive measures can be taken.

2.3.4. Threat Intelligence Sharing

Big data analytics can support the sharing of threat intelligence among multiple organizations or agencies. By anonymizing and securely transmitting threat intelligence data, different organizations can share real-time threat intelligence and work together to address a wider range of cyber threats.

2.3.5. Intelligence Prediction and Early Warning

By analyzing large-scale historical threat intelligence data, prediction models can be built to predict possible future threat trends and attack methods. Based on the prediction results, defense preparations can be made in advance to strengthen network security protection.

2.3.6. Threat Intelligence Visualization

Big data analysis technology can convert complex threat intelligence data into visual charts and images to help security

personnel understand the posture and trends of network threats more intuitively. Through visualization, it can better guide security decision-making and emergency response.

In summary, the application of big data analysis technology in threat intelligence can improve the collection, integration, analysis and application of threat intelligence. Through in-depth analysis and mining of a large amount of threat intelligence data, potential network threats can be identified more accurately, thus helping security personnel to take appropriate defensive measures early to protect the security of computer networks. At the same time, the sharing and prediction of threat intelligence can also promote the collaboration and cooperation of the network security community to form a stronger threat response force.

3. Improved Computer Network Security Prevention Program

3.1. Construction of Multi-Level Network Security Defense System

With the arrival of the big data era, computer networks are facing more complex and diverse security threats, and the traditional single security defense means can no longer meet the growing security needs. Therefore, the construction of a multi-level network security defense system has become an effective strategy to protect network security. Multi-level network security defense system improves network security and stability by combining a variety of security technologies and means to comprehensively protect the network from different dimensions.

The following are the key points for the construction of multi-level network security defense system:

3.1.1. Perimeter Defense Layer

The perimeter defense layer is located at the border of the network, and as the first line of defense, it is mainly used to prevent unauthorized access and attack traffic from entering the protected network. Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can be deployed in the perimeter defense layer to monitor and analyze the incoming and outgoing network traffic in real time to ensure network security. In addition, the perimeter defense layer can set up access control lists (ACLs) and virtual private networks (VPNs) to restrict access to specific IP addresses, ports, or protocols, increasing network isolation and protection.

3.1.2. Authentication and Access Control Layer

The Authentication and Access Control Layer is used to ensure that users and devices on the network are legitimate and are provided with appropriate privileges and access controls. Enhanced authentication mechanisms, such as multi-factor authentication, single sign-on (SSO), etc., can be deployed in this layer to prevent identity masquerading and illegal access. In addition, network access control (NAC) technology can be used to perform compliance checking and access privilege control on devices accessing the network to prevent untrusted devices from intruding into the network.

3.1.3. Security Policy and Application Layer

The security policy and application layer is the core part of the network security defense system and is used to define and implement security policies to protect network resources and sensitive data from unauthorized access and attacks. Data encryption technology can be implemented in this layer to ensure the security of data during transmission and storage. At the same time, technologies such as access control policies, security auditing and security event management can be used to strengthen the monitoring and analysis of network behavior, and to detect and respond to security threats at an early stage.

3.1.4. Application and Data Layer

At the application and data layer, security enhancement techniques can be used to harden applications and repair vulnerabilities to reduce the attack surface and avoid application layer attacks. At the same time, data classification and segregation strategies can be implemented to separate sensitive data from non-sensitive data, thereby reducing the risk of data leakage and data tampering.

3.1.5. Security Awareness Education and Training Layer

In addition to defense measures at the technical level, the multi-level network security defense system should also include a security awareness education and training layer. Security awareness education can raise the cybersecurity awareness of employees and users, educate them on how to recognize and respond to cyber threats, and avoid security breaches due to social engineering attacks.

3.2. AI-based Intelligent Security Monitoring and Response System

In the context of big data, network security faces increasingly complex and intelligent threats, and traditional security defense means have been difficult to meet the demand for real-time monitoring and response. In order to better cope with various types of security threats, an intelligent security monitoring and response system based on artificial intelligence (AI) has become a new research direction. Such systems utilize AI algorithms and technologies to perform network security monitoring and response through automation and intelligence in order to detect threats and take corresponding measures more efficiently.

3.2.1. Powerful Data Analysis Capability

The AI-based intelligent security monitoring and response system has a powerful data analysis capability that can handle large-scale network data and log information. Through real-time monitoring and analysis of massive data, it can identify abnormal behaviors and potential threats in the network, including new types of attacks and exploitation of zero-day vulnerabilities.

3.2.2. Machine Learning Algorithms

This system uses machine learning algorithms that can learn normal behavior patterns of the network from historical data and automatically adjust the model to adapt to the ever-changing network environment. Intelligent systems based on machine learning can more accurately identify unknown threats and improve the accuracy and real-time nature of security detection.

3.2.3. Automated Response Mechanism

The AI-based intelligent security monitoring and response system not only monitors threats, but also automatically triggers the response mechanism. Through pre-set rules and policies, the system can automate corresponding defense measures, such as blocking malicious IP addresses and isolating infected devices, thus reducing the impact of security incidents on the network.

3.2.4. Threat Intelligence Integration

The intelligent security monitoring and response system can integrate data from multiple threat intelligence sources to

form a comprehensive threat intelligence database. By correlating and analyzing with real-time network data, the system can identify potential threats earlier and help security teams respond in a timelier manner.

3.2.5. Visualization Display

In order to facilitate the security team's understanding and handling of threat scenarios, the AI-based intelligent security monitoring and response system can use data visualization technology to convert complex security data into intuitive charts and images. In this way, security teams can discover and understand cyber threats more quickly and make decisions accordingly.

3.2.6. Real-time and Adaptive

Intelligent security monitoring and response system has the ability to monitor and respond in real-time, so that it can discover and respond to network security threats in a timely manner. At the same time, the system can adaptively adjust security policies and models according to changes in the network environment to maintain efficient security defense capabilities.

In summary, the AI-based intelligent security monitoring and response system is an efficient, intelligent and adaptive network security defense solution. By utilizing powerful data analysis capabilities and machine learning algorithms, the intelligent system can more accurately discover network threats and automatically take corresponding defense measures. At the same time, the system can integrate threat intelligence, visualize and display data, and improve the visibility and real-time nature of network security. Such a system provides network security teams with more efficient and intelligent means of security monitoring and response, helping to improve network security and stability.

3.3. Research on Encryption Algorithms for Enhancing Data Privacy Protection

In the era of big data, data privacy protection has become an extremely important topic. With the rapid growth and wide application of data, traditional encryption algorithms may face more challenges, such as the need for efficient encryption and decryption of high dimensional and complex data. Therefore, the research and improvement of encryption algorithms, especially the research of encryption algorithms that enhance data privacy protection, become crucial.

3.3.1. Based on Hybrid Encryption

Traditional encryption algorithms usually use symmetric encryption or asymmetric encryption, but in a big data environment, these methods may have shortcomings in performance and security. Therefore, research on algorithms based on hybrid encryption techniques has become an important direction. Hybrid encryption technology combines symmetric encryption and asymmetric encryption, which takes into account the encryption efficiency and the security of key management, and improves the level of data privacy protection.

3.3.2. Enhanced Key Management

The security of encryption algorithms is closely related to key management. In the big data environment, key management becomes more complex and critical. Therefore, researching more efficient and secure key management methods, including key generation, storage, updating and distribution, can enhance data privacy protection.

3.3.3. Improved Symmetric Encryption Algorithm

Symmetric encryption algorithms are widely used in big data encryption, but certain traditional symmetric encryption algorithms may have problems such as shorter key lengths and weaker resistance to quantum computing attacks. Therefore, improved symmetric encryption algorithms, such as the improved version of AES (Advanced Encryption Standard), are studied to improve the security and efficiency of encryption.

3.3.4. Heteromorphic Encryption Algorithm

Heteromorphic encryption algorithm is an emerging encryption technique that enables computation and querying of data while keeping it encrypted. This algorithm can operate on data in an encrypted state, which improves the flexibility and usability of data privacy protection and is especially suitable for big data analysis and processing.

3.3.5. Homomorphic Encryption Algorithm

Homomorphic encryption algorithm is a special encryption technique that allows computation on data in an encrypted state without decrypting the data. This algorithm allows operations such as addition or multiplication to be performed on encrypted data without exposing the plaintext of the data, providing new ideas for data processing and privacy protection.

3.3.6. Data Partitioning and Access Control

In addition to the encryption algorithm itself, data partitioning and access control are also important means to enhance data privacy protection. By partitioning data into multiple parts and setting different access rights, fine-grained control of data can be realized to ensure that only legitimate users and devices can access the relevant data.

4. Conclusion

Starting from the current situation and challenges of computer network security in the context of big data, this dissertation discusses the application of big data analytics in network security, as well as the intelligent security monitoring and response system based on artificial intelligence, and also examines encryption algorithms for enhancing data privacy protection. Through the discussion of these contents, we have gained insight into the impact of big data on network security and the limitations of traditional security prevention means.

In the context of big data, network security is facing increasingly complex and diverse threats, and traditional security defense means have become overwhelming. However, big data analysis technology provides us with new ideas and tools to monitor and analyze network behavior from a more in-depth and comprehensive perspective, and effectively discover potential security threats. Especially in terms of intrusion detection and behavioral analysis, the application of big data analytics technology has led to a significant improvement in network security defense capabilities.

References

[1] Lu and Ping. Research on computer network security prevention under cloud computing environment[J]. Software, 2022, 43(08):50-52.

[2] Li Huilan. Research on computer network security prevention under cloud computing environment[J]. Information and Computer (Theoretical Edition),2022,34(10):236-238.

[3] Yang Deyun. Research on computer network security prevention under the background of big data[J]. Science and Technology Economic Market,2022(05):31-33.

[4] Wang Xiewei. Research on computer network security prevention in the context of big data era[J]. Computer knowledge and technology,2017,13(29):8-9.

[5] Li Guoxin. "Internet +" period of computer network security prevention research[J]. Digital world,2017(09):104.