10.18686/aitr.v2i3.4402

Application of Big Data Technology in Network Information Security Issues

Peng Zhang, Xiaomei Tang, Mengqiao Zhang

Beijing Union University, Beijing 100101

Abstract: In recent years, the rapid development of China's economy and information technology has promoted the application of big data technology in computer information systems. However, there are still some issues in practical applications that need to be overcome. This paper summarizes experiences and studies the current application status and problems of big data technology in computer network information security, hoping to provide assistance for future practical work.

Keywords: Big Data; Network Information Security; Computer; Cloud Computing

1. Introduction

In the era of big data, big data technology has been widely applied in various industries, not only providing necessary technical support but also greatly improving work efficiency. Currently, various industries rely on computer information systems to drive their development. From this perspective, using information system computers is an inevitable way to achieve industrial and modern social development [1]. The application of big data technology in computer information systems is not only a technical support for computer systems but also a key guarantee for their continuous development.

2. Big Data Technology in Computer Network Information Security

The application of big data technology in computer network information security mainly includes two aspects: cloud computing technology and data backup technology.

2.1 The Role of Cloud Computing Technology in Computer Network Information Security

As an important component of big data technology, cloud computing technology has been widely applied in our daily life and work. Its core concept is to centrally manage and dispatch computing resources through the internet, thereby achieving efficient utilization and on-demand allocation of resources. In the field of information security, the application of cloud computing technology is mainly reflected in the following aspects:

Cloud computing technology provides powerful computing and storage capabilities, making large-scale data processing possible. Through cloud computing platforms, massive network data can be monitored and analyzed in real-time, enabling timely detection and response to potential security threats. For example, cloud computing can monitor network traffic, identify abnormal traffic, and promptly alert to prevent network attacks [2].

The elastic scalability of cloud computing technology ensures network information security. Traditional computing resource configurations often encounter bottlenecks, making it difficult to cope with sudden large-scale network attacks. Cloud computing technology can dynamically adjust computing resources based on actual needs, ensuring the stable operation of network systems. This flexible resource scheduling mechanism gives cloud computing technology significant advantages in handling large-scale network attacks.

Cloud computing technology improves system security through virtualization. Through virtualization, computing resources are abstracted into multiple virtual machines, each of which is isolated and operates independently. If one virtual machine is attacked, other virtual machines and the host system remain unaffected, thereby enhancing the overall security of the system.

2.2 The Application of Data Backup Technology in Computer Network Information Security

In network information security, data backup technology also plays an important role. The core idea of data backup technology is to regularly back up important data to prevent data loss due to hardware failures, software errors, or network attacks [3]. The application of data backup technology in information security is mainly reflected in the following aspects:

Data backup technology provides a guarantee for data recovery. In the event of a network attack or system failure, the system can be

quickly restored using backup data, reducing business interruption time and data loss. This is particularly important in industries such as finance and healthcare, which have extremely high requirements for data security.

Data backup technology enhances data security through multiple backup strategies. Traditional data backup methods often use single backups, which risk losing backup data. Modern data backup technology employs multiple backup strategies, backing up data to multiple storage media and locations, ensuring that even if one backup medium fails, other backups can still restore the data.

Data backup technology can also be combined with cloud computing technology to achieve remote and off-site backups. By backing up data to the cloud, off-site storage of data can be achieved, preventing data loss due to local disasters. Additionally, cloud-based backups offer high reliability and high availability, further enhancing data security.

3. Current Application Status of Big Data Technology in Computer Network Information Security

Big data technology has shown its powerful potential and practical effects in computer network information security. With the acceleration of informatization, various security threats are becoming more complex and diverse[4]. To address these challenges, enterprises and institutions are introducing big data technology to enhance their network security protection capabilities.

Currently, the application of big data technology in network information security is mainly focused on real-time monitoring and analysis. Security systems collect and process a large amount of network traffic data and use advanced analytical techniques for real-time monitoring, quickly identifying and responding to potential security threats. For example, through big data analysis, systems can detect abnormal behavior patterns in the network and improve the accuracy and speed of threat detection through deep learning algorithms. Behavior-based threat detection systems can also effectively identify unknown threats, compensating for the deficiencies of traditional signature detection methods.

Big data technology also plays an important role in post-event analysis and tracing of security incidents. Detailed data analysis of attack behaviors can reveal the methods, tools, and paths used by attackers, helping security experts to deeply understand the attack chain and formulate more effective defense strategies. Specifically, big data-based security analysis platforms can integrate multiple data sources, including network traffic logs, system logs, and user behavior data, to reconstruct the attack process from multiple perspectives, providing strong support for forensic and tracking of security incidents.

4. Specific Applications of Big Data Technology in Computer Network Information Security Issues

4.1 Establishing a Network Information Security Service Platform through Big Data Technology

Building an efficient information security service backend is fundamental to ensuring network security. Big data technology plays a key role in this process. Modern security systems need to handle massive network data, including traffic data, log data, and user behavior data. The integration and analysis of these data rely on the powerful processing and analytical capabilities of big data technology. In practical applications, the security service backend uses big data platforms to achieve real-time processing and analysis of massive data. For example, using big data technology, a comprehensive security monitoring system can be established to deeply analyze every data packet in the network, promptly identifying potential security threats. Meanwhile, through machine learning algorithms, the security service backend can continuously optimize threat detection models, improving the accuracy and efficiency of detection[5].

4.2 Practical Application of Cloud Computing Technology in Network Information Security

Cloud computing technology has been extensively applied in the field of information security. Its core advantage lies in providing powerful computing capabilities and flexible resource scheduling mechanisms, enabling cloud computing platforms to efficiently process large-scale security data.

The distributed architecture of cloud computing platforms allows them to handle and store massive data, enhancing data processing efficiency through large-scale parallel computing. For example, security systems can use cloud computing platforms to analyze network traffic in real-time, promptly detecting and responding to security threats.

The elastic scalability of cloud computing enables dynamic adjustment of computing resources according to demand, ensuring the stable operation of the system when facing large-scale network attacks. This flexible resource scheduling mechanism gives cloud computing technology a significant advantage in handling sudden security incidents.

The application of virtualization technology in cloud computing improves system security. Through virtualization, computing resources are abstracted into multiple isolated virtual machines, each operating independently. If one virtual machine is attacked, the other virtual machines and the host system remain unaffected, thereby enhancing the overall security of the system.

4.3 Practical Application of Data Backup Technology in Network Information Security

Data backup technology is an important means of ensuring information security, preventing data loss due to hardware failures, software errors, or network attacks through regular backups of critical data. In the big data environment, data backup technology has further developed.

Modern data backup solutions support multiple backup strategies, backing up data to multiple storage media and locations, ensuring that even if one backup medium fails, other backups can still restore the data. This multi-backup strategy enhances the security and reliability of data. The application of remote and off-site backup technology allows data to be stored in multiple data centers in different geographical locations, preventing data loss due to local disasters. Additionally, cloud backups offer high reliability and availability, further enhancing data security.

4.4 Predicting Information Technology Security Trends Using Big Data Technology

Through big data technology, historical data can be deeply analyzed to identify potential security threats and development trends. This predictive capability helps to proactively mitigate security risks and guide the formulation and optimization of security strategies[6].

Big data technology can analyze network traffic and security event logs, identifying patterns and trends of network attacks, providing decision support for security experts. For example, by analyzing historical data, it is possible to identify the frequent occurrence of certain types of attacks during specific time periods, allowing for proactive protective measures.

4.5 Application of Hadoop Technology in Network Information Security

Hadoop, an open-source big data processing framework, has broad application prospects in network information security. Its distributed computing and storage capabilities allow it to efficiently handle large-scale security data. Utilizing Hadoop, a distributed security monitoring system can be constructed to comprehensively analyze network traffic and log data. Hadoop's distributed storage and computing capabilities enable it to process massive data, enhancing the accuracy and real-time detection of threats. Hadoop can also leverage various tools within its ecosystem (such as Hive, Pig, etc.) to deeply analyze and mine security data, uncovering hidden security threats and abnormal behaviors.

5. Conclusion

The application of big data technology in network information security not only improves the efficiency of threat detection and response but also plays an important role in predicting future security trends and optimizing defense strategies. In the future, with the continuous development and application of big data technology, network information security will be further enhanced and safeguarded.

References

[1] Qian Zuliang, Zhu Tieliang. Application of Big Data technology in Computer Network Information Security -- Review of Computer Network Information Security [J]. Applied Chemical Industry, 2019, 53(2):I0004.(in Chinese)

[2] Wang Lin.Application of big data and Intelligent control technology in computer network information security system [J]. Journal of Integrated Circuit Applications, 2018, 41(4):292-293.(in Chinese)

[3] She Caigao, Tang Dehao, Yu Le. Application of information management technology in Network security [J]. Communications World, 2019, 31(3):48-50. (in Chinese)

[4] Sun W. Application of big Data technology in Network security analysis [J]. Shihezi Science and Technology, 2024(2):17-19. (in Chinese)[4]

[5] Du M. Application of information communication network security management and control based on big data technology[J]. International Journal of Communication Systems, 2022, 35(5): e4643.

[6] Chen G, Wu S, Wang Y. The evolvement of big data systems: from the perspective of an information security application[J]. Big Data Research, 2015, 2(2): 65-73.