ESP-IJACT
ESP International Journal of Advancements in Computational Technology
ISSN: 2583-8628 / Volume 2 Issue 2 May 2024 / Page No: 62-66
Paper Id: IJACT-V2I2P109 / Doi: 10.56472/25838628/IJACT-V2I2P109

Original Article

Network Security Issues in the Era of Big Data

Ts. Narangerel
University of the Humanities, Ulaanbaatar, Mongolia.

Received Date: 10 March 2024 Revised Date: 12 April 2024 Accepted Date: 11 May 2024

Abstract: *The rapid development of information technology allows users to work in the networked environment of the Internet, and a large amount of information and data is created every day, which indicates the transition to the data era. Networks and information systems have become indispensable elements in the economic development of society. Network attacks are encountered at all layers of computer networks and pose risks to society, economy, and public interest. To ensure the security of the computer network, researching and strengthening the detection of cyber-attacks is the basis for ensuring the control of hardware and building a network security system. This research aims to analyze big data and network security models and intrusion detection systems and the main issues facing computer network security. A security approach should be aimed at mitigating security issues, preventing potential threats, and ensuring network security.*

Keywords: *Attacks, Viruses, Privacy, Analytics, Information, Hardware, Risk, Layer.*

I. INTRODUCTION

With the development of information technology, users can get and use the information they want based on their needs, and this use is increasing.[1] Nowadays, organizations use big data for data support and data analysis at the decision-making level, while individuals are increasingly using big data for financial, business, and research purposes in the network environment. The expansion of the use of big data in computer networks has broken the traditional model and created a completely new model of social and economic development. [2].

Thus, as computer network technology has become a major component of society, economy and life under the influence of big data, the problem of attacks in the network environment has become more and more pressing. In other words, the random distribution of information with a large number of viruses on the network poses a great hidden threat to the security of the computer network.[3].

In recent years, Internet-based e-business applications have allowed organizations to streamline processes, reduce operating costs, and increase customer satisfaction. Such applications can be used to transmit audio, video, and embedded information, and as the number of users grows, so do the network resources. As more applications are introduced to the network and more users are able to access it, there is a rise in risk to network security. Therefore, security technology plays a key role in combating threats and using electronic services without risk.

Nowadays, computer network security not only faces threats from traditional network security issues such as network viruses, hacker attacks, and network system vulnerabilities, but also the increasingly sophisticated attacks from big data and cloud computing, which is why computer network security technologies are becoming more and more sophisticated increasing in relevance. In order to keep the computer network safe and stable for a long time, it is important to analyze the security of the computer network and take certain measures to prevent and control the risks. [4].

II. NETWORK INTRUSION DETECTION IN THE BIG DATA ERA

The rapid growth of data creates major challenges and opportunities for all industries. Network big data refers to the large data available on the Internet, created by the interaction of "people, machines, and objects" in cyberspace. Big data on the network is processed by computers, regardless of space or complexity. [5]. According to the International Information Corporation, worldwide data will grow by 61% to 175ZB (Zettabyte, ZB) by 2025, and most of that data will be in the cloud as well as in data centers.

In the era of big data, computer network security faces various risks. The order of these risks may vary depending on the situation and organization, but the common security risks in computer networks are listed in order of general importance.

- *Unauthorized Access:* Unauthorized access to the network by people is a major security risk. Its purpose can be to hack, steal or use data and information.

- *Malware and Ransomware Attacks:* Malware poses a significant risk to computer networks. Ransomware is a type of malware that encrypts data and demands a ransom to release it. These attacks can cause operational disruptions, data loss, and financial losses.
- *Insider attacks:* Insiders with network access, such as employees and contractors, can intentionally or unintentionally cause security breaches. Implementing proper access control and monitoring systems and security awareness training is critical to mitigating this risk.
- *Distributed Denial of Service (DDoS) Attacks*: DDoS attacks overwhelm network resources with massive requests, rendering the network unusable for legitimate users. These attacks can disrupt operations, affect service availability, and result in financial losses.
- *Lack of encryption:* Inadequate or incomplete encryption of data during transmission may expose it to unauthorized access. Implementing encryption protocols helps ensure data privacy and integrity.
- *Inadequate monitoring and logging:* Inadequate monitoring and logging mechanisms prevent timely detection of security breaches. Implementing reliable monitoring and logging solutions is critical to detecting and responding to threats.

Network big data research currently focuses on three aspects: network big data cleaning, storage, and analysis. Network big data was mainly used in fields such as communication monitoring, modeling, keyword research, information engineering, etc., but today it is used in all fields for more effective processing, increasing the value of information, and distributing it in a form that is easy for people to use. [6].

A. Network Security Model

With the continuous increase of the information process and the rapid development of network technology, the problem of network security is increasing, and the security of multi-layer three-dimensional network architecture is becoming more and more sophisticated.[8].

The basic requirements of computer network security are availability, integrity, confidentiality, control and reliability. The concept of computer network security consists of three parts: network platform operational security, physical security, and security management. At the core of these is physical security, which ensures the operational safety and security management of the network platform. Together, they form a relatively complete system of network security protection. (Figure 1).

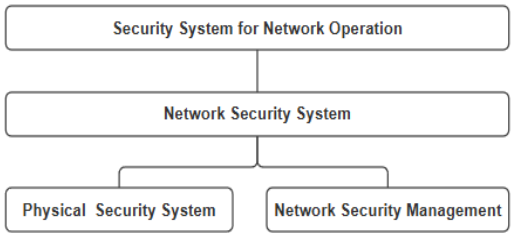

Figure 1: Network Security System

B. General Structure of Network Attacks

A network attack is an abstract concept. Network attacks cause certain damage to network resources, and these damages are divided into the main types: first, loss of integrity of network resources, second, destruction of network resource availability, and third, destruction of confidentiality of network resources. These malicious activities can cause network security problems. Network attacks can be divided into masquerade attacks, denial of service attacks, security level update attacks, and attempted attacks. (Figure 2).

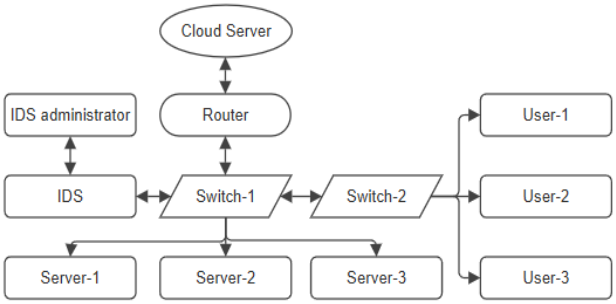

Figure 2: Basic Attack Detection System

The main purpose of this system is to detect possible or previous attacks on the network, and then to respond to the attack. Intrusion detection focuses on analyzing network data and conditions by analyzing active security technologies and related problems such as network devices, hosts, logs, etc. in the event of a network attack and, if necessary, destroys network resources to prevent the attack. The basic principles of intrusion detection are analysis of network intrusion activity, network logs, and audit logs. The intrusion detection system has the following functions: Helps the system administrator to understand network system hardware and software changes, operating modes, communication changes, etc.

An intrusion detection system monitors and manages the network. The network administrator can make network security settings through the intrusion detection system to improve the security of the network system. An intrusion detection system must be able to respond quickly. When an attack is detected, the system logs the malicious activity in a timely manner, allowing you to take action, such as removing network connections and alerting the administrator.

Network intrusion detection works by analyzing information transmitted over the network between hosts. For example, it is possible to monitor and analyze the flow of data passing through websites with illegal information in real time. Its analysis module usually uses methods such as statistical analysis in its appropriate form to determine the level of attack during an attack. (Figure 3).

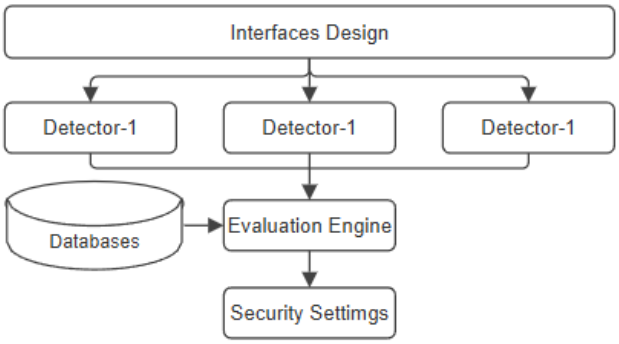

Figure 3: Structure of a web-based intrusion detection system

III. ANALYZING NETWORK SECURITY ISSUES

As countries, organizations, and specific industries use big data processing technology based on their own needs, and strive to make more reasonable and scientific decisions, security in the network environment has become more and more pressing. Although consumers understand the importance of network security and take preventive measures, they are still not very effective.

A. Unlawful Attack

Because the network is an open system that allows space to be used independently, attackers can gain access to the network. As the amount of data increases, the security in the network environment loosens to a certain extent. If traditional computer network security technologies are used, it is difficult to detect hacker attacks, and various information is greatly increased in the network environment to hide the hacking activity. Hacking often results in data loss. With the development of Internet technology, viruses are becoming more sophisticated and powerful. Viruses are one of the main risks for computer network security. If a virus infects a computer, even if the computer is working normally, the virus will continue to spread to other links in the computer, which in turn can paralyze the entire computer system.

B. The Policy and Regulatory Framework is Imperfect

Countries continue to issue their own information security policies and legal acts. Despite the legal requirements for the use of big data in our country, the issue of data security is still important. The fact that most countries are investing in the field of information security shows that our country needs to consider the issue of information security and strengthen it, and it is necessary to pay more attention to the implementation of policies and regulations on information security.

It is important that all levels of management, from the enterprise level, understand the importance of network security and take appropriate measures. Some users, especially at the enterprise level, lack reliable systems to prevent and monitor network intrusions, increasing hidden network security threats. At the organizational level, network security control systems vary. This is due to the organization's lack of network management expertise and the inability to detect many security risks, which compromises network security.

C. Knowledge of network security is weak

Even after a network attack occurs, there is still a lack of real-world effectiveness of measures and maintenance. Network security can only be better achieved by properly securing sources and consciously configuring security at the beginning of data generation. However, there is currently a lack of security awareness among network administrators and ordinary users. For example, many websites have simple login password settings, and users often use the same password when logging in with different software. Some users do not set their security passwords at all, which creates hidden security risks.

III. SECURITY MEASURES TO IMPROVE NETWORK SECURITY

A. Prevent Illegal Attacks through Computer Network Monitoring Technology

Network companies, government agencies and other places must continuously improve their computer network monitoring technology and adopt intelligent network monitoring technology. Since the entire computer network cannot be controlled by people all the time, it is necessary to use intelligent control technology. Monitoring technology can be used in the development and operation of system programs to prevent illegal attacks, in addition to building virus attack databases and monitoring models.

Re-encoding the data before transmission prevents the original content of the data from being compromised. Data encryption technology is a basic security technology in computer networks, which guarantees the safe transmission of data. In data encryption technology, methods such as symmetric key encryption and asymmetric key encryption are used, each of which has its own advantages depending on the specific application requirements.

When transmitting large amounts of data in a network environment, performing encryption using an asymmetric algorithm is relatively reliable in terms of computation, although the speed of the asymmetric algorithm is relatively slow compared to the symmetric algorithm. Asymmetric key encryption is usually used to encrypt large amounts of data, while symmetric key encryption is used for small amounts of data.

Asymmetric key encryption is the most widely used method for large data transmission, and its security is higher than that of symmetric encryption. It uses a pair of related keys, one of which is a public key and the other is a private key. Currently, relatively secure asymmetric encryption algorithms include RSA, DSA, PKCS, and PGP. (Figure 4).

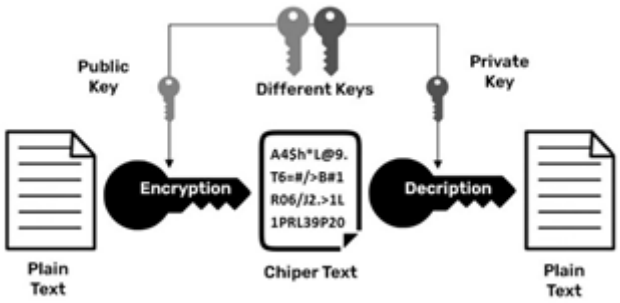

Figure 4: Schematic Diagram of Asymmetric Encryption

B. Strengthen Awareness of Computer Network Security

As the use of the Internet increases, individuals also need to be more IT literate. Network security issues are directly related to people's ignorance, irresponsibility, and lack of legal understanding. Not only are individuals vulnerable to network attacks themselves, but they also put the security of others at risk.

It is important to increase users' awareness of computer network security protection, the dangers of illegal attacks, and preventive measures. For example, learn to use a high level of security combination when setting up your username and password - use a combination of symbols, letters and numbers, do not use the same password for different websites, and learn to use methods such as changing your password regularly. On the other hand, access rights should be limited as much as possible so that each user has their own access rights. When using public networks and public WIFI, you should avoid accessing certain software and websites that contain your private or sensitive information.

IV. CONCLUSION

Due to the high degree of freedom in computer networks in the context of big data, many problems related to network security arise. This article first briefly analyzes the main network security issues and finally offers appropriate solutions for common problems. In the first place, it is important to improve the policy and regulatory environment aimed at protecting and ensuring security of information in computer networks, and to pay attention to improving implementation at

all levels. However, it is important to introduce new security technology solutions at the level of organizations and ordinary users, but no matter how good security technologies and programs are introduced, in the end, individual knowledge and responsibility are the most important to ensure network security. Therefore, it is necessary to regularly take and implement measures aimed at increasing public understanding and required skills about working safely in computer networks.

V. REFERENCES

[1] Ts. Narangerel., University of the Humanities, Internet commerce security issues in wireless networks. Scientific journal, no. 01(19), 415-422, 2019

[2] Yang, J.W., A brief analysis of computer network security precautions in the era of big data. Science and Technology Communication, no.2, pp.108-109, 2019.

[3] Long, Z.H., Computer network information security and protection strategy in the era of big data. Management Informationization in China, no.3, pp.161-162, 2019.

[4] Deng, Q.F., Computer network information security technology and its development trend. Electronic Technology and Software Engineering, no.24, pp.194-195, 2019.

[5] Liu, W, Research on Optimizing Network Security Strategy Based on Big Data. Software, vol.39, no.9, pp.205-208, 2018.

[6] L.Zhao, “Research on computer network security protection strategy under the background of big data.” *Journal of Heihe University,* vol.10, no.1, pp.217-218, 2019.

[7] Wang, Q., Pan, C., Analysis of Network Complete Vulnerabilities and Preventive Measures in the Era of Big Data. Network Security Technology and Application, no.2, pp.77+ 79, 2017.

[8] Bao, L.J., Application of Big Data-based Network Security Situation Awareness Platform in Private Network Field. Information Security Research, vol.5, no.2, pp.168-175, 2019.

[9] Wang, B., Network security fuzzy risk assessment based on computer network technology. Foreign Electronic Measurement Technology, vol.38, no.5, pp.11-16, 2019.

[10] Liu, Q., Cai, Z.P., Yin, J.P., et al., Research on the framework and methods of network security detection. Computer Engineering and Science, vol.39, no.12, pp.2224-2229, 2017.

[11] B. Namatherdhala, A. Ganesh, N. Memon and J. Logeshwaran, "The smart detection of neuro-pathological effects of alzheimer patients using neural networks," 2023 *Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Singapore, Singapore, 2023, pp. 858-863, doi: 10.1109/SmartTechCon57526.2023.10391384. | Google Scholar