ISSN 2616-5775 Vol. 6, Issue 3: 123-128, DOI: 10.25236/AJCIS.2023.060316

Network Security Technology and Application in the Era of Big Data

Jiana Bi*, Yonghong Guo

School of Software and Big Data, Changzhou College of Information Technology, Changzhou, China
544099426@qq.com
**Corresponding author*

Abstract: *The network has a strong openness, which can realize the communication and interaction across time and space, but it is also vulnerable to different intrusions and attacks, which leads to the leakage of data information and serious network security problems. Big data increases the complexity of computer network, which makes the security problem of computer network more prominent. Based on a comprehensive analysis of computer network security issues in the era of big data, it is of great significance to deeply explore specific network security technologies. Based on the WPDRRC network security model, this paper studies the network security technology and application in the era of big data, including virus protection technology, intrusion detection technology and access control technology. In practice, it is necessary to formulate a more secure network protection system, create a healthy and green network environment, and meet the needs of network security in the era of big data.*

Keywords: *Big Data Era; Network Security; Technology and Application; Virus Protection Technology; Intrusion Detection Technology; Access Control Technology*

1. Introduction

Network security means that the hardware and software of the network system and the data in the system are protected from being damaged, changed and leaked due to accidental or malicious reasons, and the system runs continuously, reliably and normally without interruption of network services. Network security is essentially network information security. Generally speaking, all related technologies related to the confidentiality, integrity, availability, authenticity and controllability of network information belong to the field of network security research. Network security involves computer science, network technology, communication technology, cryptography technology, information security technology, applied mathematics, number theory and information theory.

Big data refers to a collection of data that cannot be captured, managed and processed by conventional software tools within an affordable time range. A new processing mode is needed to have a huge, high growth rate and diversified information assets with stronger decision-making, insight and process optimization capabilities. Big data is considered to be another peak of the whole information revolution after informationization and Internet, which is characterized by abundance, high speed, diversity, value, variability and authenticity [1].Big data is a new production factor, and its usage tends to be user behavior analysis, predictive analysis or other advanced data analysis methods. In the era of big data, any tiny data may produce incredible value.

In the era of big data, computer networks have achieved a leap in "quality" and "quantity", which has driven the rapid development and progress of many industries. At the same time, big data has also increased the complexity of computer networks, resulting in outstanding computer network security issues, and increasingly intensified. This gives some offenders an opportunity to use computer networks to steal user information and commit online fraud, which has a bad social impact and has attracted widespread attention [2].In order to ensure the security of computer network, it is necessary to start with the current situation of computer network environment under the background of big data, analyze common computer network security problems, find out the root causes of the problems, and formulate relevant strategies.

ISSN 2616-5775 Vol. 6, Issue 3: 123-128, DOI: 10.25236/AJCIS.2023.060316

2. Network Security Architecture Model: WPDRRC

PDR, P2DR, PDR2 and PDR2A are the representatives of the dynamic adaptive security model. The basic idea is to allow the system to have security vulnerabilities to a certain extent, and to eliminate network system vulnerabilities as much as possible, while emphasizing the timely discovery of attacks and real-time elimination of security risks. Among them, PDR model is the earliest network security model that embodies the idea of active defense, and it is the cornerstone of other network security models in the later period. Under the control and guidance of the overall security policy, P2DR model comprehensively uses protection tools and detection tools to understand the security state of the system, and adjusts the system to the safest and lowest risk state through appropriate means. PDR2 model is a dynamic technical system combining protection, detection, response and recovery. The PDR2A model is based on the original PDR2 security model, and an audit analysis module is added.

WPDRRC network security model is a network security model which is put forward by Chinese 863 information security expert group on the basis of PDR model, P2DR model, PDR2 model and PDR2A model and is suitable for Chinese national conditions. The WPDRRC network security model has the advantages of comprehensive functional coverage and wide application range, and truly achieves the seamless integration of technical means and management means. The structure of WPDRRC network security model is shown in Figure 1 [3-5].

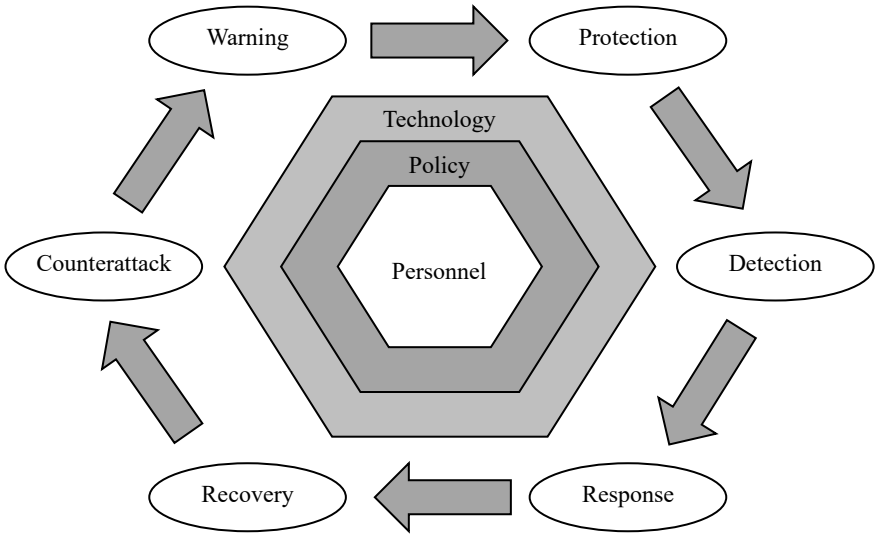

Figure 1: Network security architecture model: WPDRRC

The WPDRRC network security model consists of three elements and six links. The three elements are personnel, strategy and technology from the inside out. Among them, people are the central link of information security, and strategies are policies, laws and regulations that connect people with technology. Technology runs through six links to ensure the realization of security goals. The six links, including early warning, protection, detection, response, recovery and counterattack, have strong time sequence and dynamics, which can better reflect the early warning ability, protection ability, detection ability, response ability, recovery ability and counterattack ability of the system security system.

WPDRRC network security model, like most security models, is also based on time theory. D_t is the time required for the detection system to discover the attack behavior when the attack occurs, and R_t is the time required for the response link to start. E_t is the recovery time, and P_t is the time required for the attack to succeed. When $P_t = D_t + R_t$, that is, when the attack success time is greater than the detection time and the system response time, the system is safe.

3. Network Security Technology and Application in the Age of Big Data

Network security technologies and applications in the era of big data include many contents. This paper mainly studies virus protection technology, intrusion detection technology and access control

ISSN 2616-5775 Vol. 6, Issue 3: 123-128, DOI: 10.25236/AJCIS.2023.060316

technology.

3.1 Virus Protection Technology

Computer virus refers to a set of computer instructions or program codes inserted by a compiler in a computer program that destroys computer functions or data, affects the normal use of the computer and can replicate itself. Computer viruses are contagious, hidden, infectious, latent, excitable, expressive or destructive. Computer virus is man-made, destructive, contagious and latent, and has a destructive effect on computer information or systems. Computer viruses are artificially produced and spread, and they are highly concealed in the process of spreading. It is not easy for ordinary computer users to find the existence of network viruses. Therefore, the information resources and files existing in computers are easily destroyed or stolen [6]. The main routes of virus transmission are shown in Table 1.

Table 1: The main route of virus transmission

No	Main route
1	The computer hardware equipment, including ASIC chips and hard disks, etc.
2	Mobile storage devices, including floppy disks and tapes.
3	Computer network is the most important way of communication at present.
4	Point-to-point communication system and wireless channel propagation.

(1) Establish an effective virus protection mechanism [7]. When using a computer, it is necessary to install defensive software such as firewall and antivirus software. When browsing a webpage with virus codes, downloading software and files with viruses, or being maliciously attacked by hackers, the installed anti-virus software or firewall will play a role in preventing hackers from attacking, identifying viruses in time, preventing viruses from spreading and eliminating them, so as to provide a layer of security for computers and improve the overall security performance of computers.

(2) Install file patches regularly. File patch is to directly modify the binary data of executable files. It is necessary to regularly test computer software, install the latest version of patches in time, and repair problems in computer systems in time. The patch itself may also have some defects, which may sometimes lead to computer system problems or even direct crashes, but most of the reasons for such problems are pirated software downloaded by users or viruses carried by themselves.

(3) Pay attention to emails from unknown sources. There are various forms of e-mail sent on the Internet, and there are no strict restrictions on the sender. Many unscrupulous people use e-mail to send advertisements, pictures, links or files to users, which often become the carrier of viruses. When users open these files, viruses will quickly infect computers. Therefore, we must be careful to receive emails from unknown sources. Therefore, emails from unknown sources must be carefully received. When opening emails or attachments, it is necessary to ensure that firewalls and anti-virus software operate normally.

3.2 Intrusion Detection Technology

Intrusion detection technology is a kind of network security technology that actively protects against attacks. As a reasonable supplement to firewall, intrusion detection technology can help the system cope with network attacks, expand the security management ability of system administrators and improve the integrity of information security infrastructure. Intrusion detection methods include monitoring and analyzing user and system activities; Audit of system structure and weakness; Identify the activity pattern reflecting the known attack and give an alarm; Statistical analysis of abnormal behavior patterns; Evaluate the integrity of important systems and data files; Audit tracking management of operating system, and identify users' behaviors that violate security policies. The workflow of intrusion detection technology is shown in Figure 2 [8].

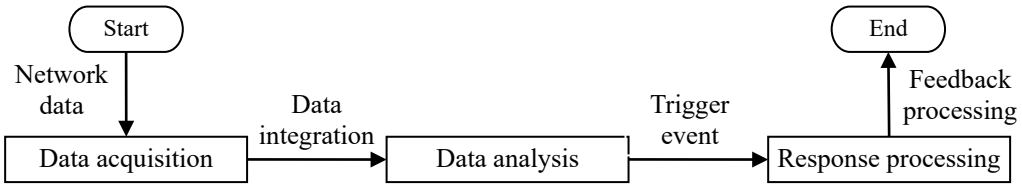

Figure 2: Working process of intrusion detection technology

ISSN 2616-5775 Vol. 6, Issue 3: 123-128, DOI: 10.25236/AJCIS.2023.060316

For the working process of the intrusion detection technology shown in Figure 2, there are three processes. Collecting data and information in the network; Comprehensively analyze and sort out the collected information; Make an appropriate response through the analysis results, and feed-back the processing results of the response, that is, send out the corresponding alarm or stop behavior to ensure the normal operation of the network system. Network intrusion detection technology needs to adapt to the new development trend, including three aspects [9].

(1) Detection technology in more innovative. With the development of network technology, the danger of intrusion is getting higher and higher. In order to ensure network security, new detection technology must be adopted. The distributed IDS technology can be used to extract data from the computer network, and a new detection model can be established by using various detection methods. Cloud computing technology can also be used to realize the intelligence of computer technology and reduce the detection cost.

(2) Detection methods are more abundant. In real life, there are many ways of intrusion, which can't be found in time and can't guarantee the network security. Therefore, only by improving the detection technology in time can we ensure the network security.

(3) Detection method is more intelligent. With the rapid development of science and technology, there are more and more forms of intrusion, and the current intrusion detection technology has been unable to adapt to the development of the network and cannot find the intrusion in time. Therefore, in improving the security and intelligence of computer network, many intelligent intrusion detection technologies promoted in recent years include fuzzy technology, neural network and genetic algorithm. Taking fuzzy technology as an example, it can eliminate the barriers of traditional intrusion detection technology and firewall sharing defense, improve computer network security, and prevent network security problems caused by firewall problems [10].

3.3 Access Control Technology

Access control refers to the subject's different authorized access to the object itself or its resources according to some control policies or permissions. On the basis of identity authentication, access control is to control the resource access request according to identity, which is a defensive measure against the phenomenon of unauthorized use of resources. Access control is the main strategy of network security prevention and protection, which can restrict access to key resources and prevent damage caused by careless operation by illegal users or legal users. The principle of access control is shown in Figure 3.

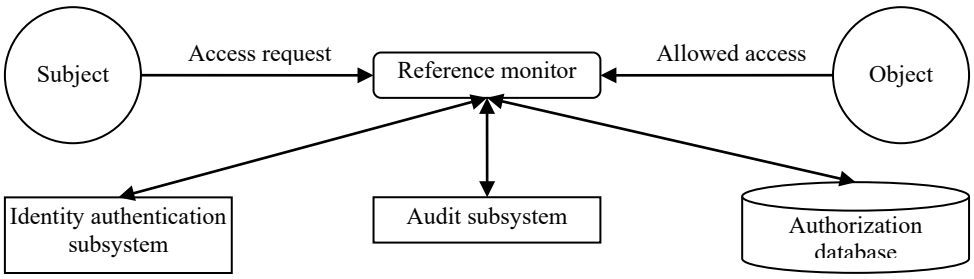

Figure 3: Access control principle

(1) Autonomous access control policy [11]. In the working system of computer application, autonomous access control is a common and widely used processing control mechanism. After the computer application subject establishes the corresponding control structure, it actively authorizes the receiver to ensure effective access to the subject, mainly using DAC system to establish a complete system access control structure. It is this structure that ensures the corresponding degree of the main body of the system, and the related factors indicate the access authority of the main body to the object, which can improve the running performance of the system. During the operation of DAC system, access rights are set according to the actual identity of users, which improves the flexibility of control structure. Therefore, it is widely used in commercial fields, and the control of operating system and relational database is more effective.

(2) Mandatory access control policy [12]. In the autonomous access control system, because it cannot effectively resist strong Trojan attacks, it is necessary to use mandatory access control policies

ISSN 2616-5775 Vol. 6, Issue 3: 123-128, DOI: 10.25236/AJCIS.2023.060316

to supervise access. The early compulsory access control system was mainly used in communication system and interactive mode, which deeply controlled access rights, supervised information and supervised access according to the permission of hierarchical list, and effectively restrained some illegal intrusions. Mandatory access strategy also has some disadvantages. If users maliciously disclose information, the overall security of the system will be seriously affected. In addition, the regulatory mandatory access control system increases the confidentiality of information interaction, but it cannot establish a complete regulatory control structure, making the system security loopholes still obvious.

(3) Role access control policy. Under the background of the continuous development of computer network technology, the frequency of computer application increases, and the demand for information integrity exceeds the demand for information security, which leads to the traditional independent access strategy and compulsory access strategy cannot meet the actual needs. Role-based access control strategy can establish more authoritative data and information control models, mainly including RBAC reference model and RBAC function planning system, which creates a good platform for system function research and development and review management. At present, role-based access control strategy is mainly used in operating system, database management system, industrial process management system and other fields, which ensures the rationality and scientificity of standardized operation on the basis of improving system operation efficiency.

4. Conclusions

Under the background of the era of big data, there are many problems in computer network security, such as insufficient awareness of prevention, backward technical level and imperfect institutional mechanisms, which seriously affect computer network security. In order to keep pace with the development of the times, the government, enterprises and individuals should be deeply aware of the importance of computer network security, and improve the level of computer network security by strengthening computer network security awareness, upgrading computer network security technology, improving computer network security mechanism and other measures, so as to provide a strong guarantee for the development of various industries and national economic construction.

Acknowledgements

This work is supported by Jiangsu innovation and entrepreneurship doctor project: Research on personal information security protection protocol in big data; Natural Science Foundation of Changzhou College of Information Technology (CXZK202004Y): Research on the model and service discovery mechanism for the future distributed social network; Scientific Research and Development Center for Colleges and Universities of the Ministry of Education, China University Innovation and Research Fund (2021LDA06008): Steel product defect detection based on big data and industrial vision.

References

[1] Y. J. Zhang, H. Y. Sun. Research on manufacturing supply chain management under big data and blockchain technology[J] .China Collective Economy, 2023, 39(05): 101-104.
[2] Y. F. Cao, H. T. Wei. Research on computer network security in the context of big data[J]. Computer Knowledge and Technology, 2022, 18(03): 34-36.
[3] S. B. Yang, L. C. Zheng, X. W. Jing. Research and design of enterprise technology security technology system framework based on WPDRRC model[J]. Secrecy Science and Technology, 2019, 10(05): 50-58.
[4] M. X. Yuan, Z. Wang. Research on security evaluation of hospital information system based on WPDRRC model[J]. Electronic Design Engineering, 2016, 24(11): 11-14.
[5] Z. Yang. Network Security Construction for University Libraries Based on WPDRRC[J]. Journal of Modern Information, 2010, 30(02): 92-94+97.
[6] J. Chen, W. Y. Ye. Study on virus protection technology in computer network[J]. Computer Knowledge and Technology, 2019, 15(01): 30-31.
[7] F. Lu. Discussion on Virus Protection Technology in Computer Network Application[J]. China Computer & Communication, 2019, 13(09): 22-24.
[8] M. P. Xu. Explore the application of intrusion detection technology in computer network security[J]. Computer Knowledge and Technology, 2022, 18(36): 75-77.

ISSN 2616-5775 Vol. 6, Issue 3: 123-128, DOI: 10.25236/AJCIS.2023.060316

[9] K. Guo. Research on Intrusion Detection Technology of Computer Network Security[J]. Network Security Technology & Application, 2023, 23(01): 7-9.
[10] Y. Wang. Application analysis of intrusion detection technology in computer network security[J]. Wireless Internet Technology, 2022, 19(14): 99-101.
[11] T. L. Liu. Access Control Technology in New Network Environment[J]. Computer Knowledge and Technology, 2019, 15(19): 40-41.
[12] W. Q. Yi. Access Control Technology in New Network Environment[J]. Computer Knowledge and Technology, 2018, 14(35): 37-38.