Research on Application of Artificial Intelligence in Network Security Defence

Qingmin Yuan, Xin Tan*
School of Management, Tianjin University of Technology, Tianjin, China
*Corresponding author: xintan2020@tjut.edu.cn

Abstract. Network security gradually matures with the development of IT technology, and the exponential growth of massive data makes data leakage more common for many reasons. To explore the application of artificial intelligence technology in network security defense. Based on the security problems existing in different network information systems, this paper constructs an intelligent security analysis and management system from the perspective of network security protection, and introduces it into the big data network security platform. In combination with different security protection requirements, the existing network security problems are detected and dealt with. The VLAN routing command is configured to multiple switches to quickly complete multiple sets of network security solutions and implementation, and achieve a more comprehensive and intelligent network security defense.

Keywords: Artificial intelligence technology, Network security defense, Big data platform, Application introduction.

1. Introduction
According to the market and market artificial intelligence network security forecast report, it is estimated that by 2026, the scale of artificial intelligence network security market will increase from US $8.8 billion in 2019 to US $38.2 billion, with an annual compound growth rate of 23.3%. The main driving force of market growth is that new attack surfaces and attack vectors often exceed the perceived range, processing capacity and response speed of traditional security defense systems, such as the popularity of the Internet of things, the increase of networking devices, the increase of network threat instances, and the increasing attention to big data privacy. Artificial intelligence based on big data and cloud computing technology, as an emerging technology, has a strong defensive role. Therefore, artificial intelligence technology is applied to big data network security defense to improve the security of big data network.

2. Security problems existing in network information system
It is generally believed that the current threats to the network mainly include: using the network to spread viruses, unauthorized access, information disclosure or loss, destroying data integrity and denial of service attacks.

Using network to spread virus refers to spreading computer virus through the network. Its destructiveness is much higher than that of single machine system, and it is difficult for users to prevent
Unauthorized access refers to the use of network or computer resources without prior consent, which is regarded as unauthorized access, such as deliberately avoiding the system access control mechanism, abnormal use of network equipment and resources, or unauthorized expansion of authority and unauthorized access to information. It mainly has the following forms: counterfeiting, identity attack, illegal users entering the network system for illegal operation, legal users operating in an unauthorized way, etc. Information leakage or loss refers to the intentional or unintentional leakage or loss of sensitive data. It usually includes the loss or leakage of information during transmission (for example, hackers can intercept confidential information by means of electromagnetic leakage or wiretapping, or launch useful information through the analysis of information flow direction, flow, communication frequency and length, such as household registration order Account number and other important information.), Information is lost or leaked in the storage medium, and sensitive information is stolen by establishing a hidden tunnel. If the integrity of data is damaged, the right to use the data is stolen by illegal means, and some important information is deleted, modified, inserted or retransmitted in order to obtain a response beneficial to the attacker; Malicious addition and modification of data to interfere with the normal use of users. Denial of service attack, which constantly interferes with the network service system, changes its normal work flow, executes irrelevant programs, slows down or even paralyzes the system response, affects the use of normal users, and even makes legitimate users excluded from entering the computer network system or unable to get corresponding services.

3. Application of artificial intelligence technology in big data network security defense

3.1. Network security situational awareness

All Network security situation awareness is the use of data fusion, data mining, intelligent analysis and visualization technology, intuitive display of real-time security status of the network environment, to provide security for network security. With the help of network security situation awareness, network supervisors can timely know the status, attack situation, attack source, and vulnerable services of the network, and take measures against the network that initiates the attack. Network users can clearly understand the security status and trend of the network and make corresponding preparations to prevent and reduce losses caused by viruses and malicious attacks on the network. The emergency response organization can also understand the security situation and development trend of the network from the network security situation, which provides the basis for formulating a prescient emergency plan.

3.2. Association rule mining technology

In the process of transmission and processing of massive complex network information, the association technology of giving rules should be adopted to comprehensively analyze the operation of equipment and data transmission in the network system, so as to master the association relationship between network security hidden dangers, alarm events and existing log data. In this process, the sequence template of network security attacks and alarm events is matched with the corresponding rule sequence of security events, and the data information and digital signatures are verified to reduce the illegal control of the network security system. Thus artificial intelligence security system planning and design departments, mainly through the establishment of public information resources acquisition interface, and the use of correlation methods such as data mining, expert evaluation, from the backend database huge amounts of data resources, extract the code associated with network security attacks, alarm event data, accurately identify the invasion risk, Form a set of security resource categories associated with the engine and store them in the background database[1].

3.3. Big data association analysis technology

Association analysis refers to the discovery of interesting associations and correlations between itemsets from large amounts of data. A typical example of association analysis is shopping basket analysis. In the era of big data, correlation analysis is one of the most common data mining tasks. In the face of network security defense of massive data, it is necessary to collect Marine, high-speed, diversified and
low-value density data resources by means of association rule mining technology. After using GBM machine learning, depth, machine learning, multi-dimensional correlation analysis, such as technology, correlation coefficient, significance test, correlation analysis category, to multidimensional, multiple source information integration analysis, timely monitoring and found that the potential vulnerabilities, security, aggression, specific component architecture is shown in figure 1.

![Figure 1. Big data association analysis module architecture](image)

Generally, Pearson correlation coefficient is adopted to carry out positive/negative correlation analysis of multiple variables for data resources with large scale and low value density, so as to make accurate judgment on alarm events and security attack problems that have occurred, and complete service operations such as security event traceability and multi-point protection in time. To realize the network security system weak links to prevent. The formula to reflect the degree of linear correlation is [2]:

$$\rho = \frac{\sum_{i=1}^{n} \left( x_i - \bar{x} \right) \left( y_i - \bar{y} \right)}{\sqrt{\sum_{i=1}^{n} \left( x_i - \bar{x} \right)^2} \sqrt{\sum_{i=1}^{n} \left( y_i - \bar{y} \right)^2}}$$

In formula (1), $r>0$ means that there is a positive correlation between the two variables; $r<0$ indicates that there is negative correlation between the two variables; $r=0$ indicates that there is no correlation between the two variables. Significance test is to calculate the correlation degree of network security events and security risks. Generally, the overall correlation coefficient is denoted as $\rho$, where $\rho<\alpha(\alpha=0.05)$ means that there is a significant linear correlation between the two variables, otherwise there is no significant correlation.

3.4. Interactive network analysis techniques
Interactive data processing is flexible, intuitive and easy to control. The system and the operator ask and answer in the form of man-machine dialogue. The data files stored in the system can be processed and modified in time, and the processing results can be used immediately. These characteristics of interactive data processing can ensure that the input information can be processed in time and make the interactive mode continue. The interactive network modeling and analysis technology of artificial intelligence is a hierarchical three-dimensional protection technology of network system. The adaptive network security model is mainly used to conduct dynamic monitoring and analysis of multiple data sources and security events in combination with different business scenarios of network security defense. Among them, firewall, dynamic / static encryption, security access authentication and other technologies are to filter the code data of multiple nodes by gathering multiple data nodes / links through the visual mapping of
the original data and the new data value generated in the background. In the face of new network security threats in different business scenarios, with the help of data information detection and security access authentication technology, as well as the prototype system and reduction algorithm of interactive network, make correct response to cross site access requests and cross site script attacks on Web sites, and analyze the potential risks of network security threats. And adjust the system to the security defense state, so as to ensure the effectiveness of security analysis and control of different enterprise website systems.

4. Application strategy of artificial intelligence technology in network security defense

4.1. Artificial intelligence platform architecture for network security defense

In the face of massive data from various sources, how to effectively analyze these scattered data and obtain valuable information has always been a hot issue in the field of big data. Big data analysis and processing platform is to integrate the current massive data analysis frameworks and tools from various sources to realize data mining and analysis. At present, the defensive platform architecture of artificial intelligence security network usually includes data acquisition layer, data preprocessing layer, data storage layer, data analysis and operation layer. Different levels not only maintain close correlation, but also are independent of each other. The specific network security platform architecture is shown in Figure 2 [3]. From the perspective of the collection, preprocessing, extraction and conversion and normalization integration process of the underlying data resources, data mining, machine learning, batch stream processing and other technologies are usually adopted to preprocess the collected massive data content. Then, according to the parallel processing, information migration and distributed storage requirements of different types of data, the received data log and table structure information are imported into NoSQL distributed database and relational database by using the distributed file system. Finally, as the analysis level of network security risks, the data analysis and calculation layer include association rule mining, real-time association analysis, interactive modeling analysis, complex security event analysis and other components. This level will first give the data and transaction set of potential security risks, and then target the existing network security attacks and alarm events, carry out intelligent association rule analysis and calculation, and mine the information correlation and confidence of different network security data, so as to facilitate the background management system to make accurate response and processing.
4.2. Security defense deployment and function realization of network artificial intelligence platform

In the process of network security defense using artificial intelligence technology, data information collection and network behavior management are mainly carried out by deploying multiple core switches to the LAN. Each core switch needs to be configured with a separate mirror port. Then, with the help of sandbox detection engine, big data real-time analysis engine and sandbox analysis module, machine learning simulation analysis is carried out for a variety of data traffic and information resources existing in the network platform to detect hidden malicious files, viruses and Trojans contained in different data.

Therefore, relying on the core switch, access switch, Wfilter host and other hardware, multiple VLAN routing execution commands are configured into multiple switches to set the network segment and port IP of Wfilter system, so as to complete the intelligent deployment of network security defense and effectively ensure the realization of user access, data transmission and business service functions. The specific network topology is shown in Figure 3. Select the Cisco 3550-layer 3 switch, set vlan2-192.168.2.0/24 and vlan3-192.168.3.0/24, set the IP address connected between the Cisco 3550 switch and the Wfilter port to 192.168.1.5, and then configure the routing rules to the VLAN in the Wfilter system to complete the security control of user access, data information transmission and response in the artificial intelligence platform.

For example, in the process of massive data collection, security alarm log collection, data information transmission, data analysis and storage, the information to be processed and the corresponding target tasks to be completed are obtained through association rule mining. Then, using real-time correlation analysis, interactive modeling analysis and other technologies, according to the set rules, the data packet...
capture of network channel and the docking between different network key nodes and business services are carried out for multiple execution tasks of artificial intelligence model, and the hidden security problems such as platform access, data use and modification, virus intrusion and so on are found in the network system. Finally, the complex security event analysis technology is adopted to carry out all-round task scheduling processing on the data log and table structure information received by the computer network platform, and output the corresponding security risk analysis results [4].

Therefore, through the application of network computer hardware, storage media, big data association analysis, interactive modeling analysis and other technologies of the artificial intelligence system, the service function of dynamic active defense can be built to deal with the existing abnormal access behavior and data transmission security risks, so as to effectively reduce the probability of malicious intrusion of the artificial intelligence system, improve the security of artificial intelligence system.

5. Conclusion
In the long-term development process, artificial intelligence has been adapting to the changes of the times, and even leading the development of the times. In order to solve the increasingly serious network security threats and challenges, it is necessary to introduce data encryption transmission technology, batch stream processing, association rule mining, batch stream processing and other technologies based on artificial intelligence to process the received data log and table structure information, and deal with the existing illegal network access, hidden dangers of data transmission and security attacks. Make intelligent association rule analysis to determine the correlation and confidence of different data information. From the perspective of network security defense, build a network intelligent security analysis and management system to accurately detect, respond, process and feedback network security events and security threats in a certain space, and configure VLAN routing execution commands to multiple switches, which can quickly complete the design and implementation of multiple sets of network security disposal schemes.

References
[1] Bai Miao, Wan Li. Exploring the application of artificial intelligence in computer network technology based on the era of big data [J]. China new communications, 2018, 20 (03): 89.
[2] Liang Jiye, Feng Chenjiao, Song Peng. Overview of big data correlation analysis [J]. Journal of computer science, 2016, 39 (01): 1 - 18.
[3] Feng Guilan, Li Zhengnan, Zhou Wengang. Research review of big data analysis technology in the network field [J]. Computer science, 2019, 46 (06): 1 - 20.
[4] Gong Zhiyuan. Analysis of computer network defense technology based on prevention strategy [J]. Digital technology and application, 2020, 38 (01): 178 - 179.