Universe Scientific Publishing

Application of Data Mining Technology in Network Security

Zijun Yang
Changzhou university of technology, Changzhou 213000, China.

Abstract: With the growing national economy and the development and progress of science and technology, computer networks have achieved all-round popularization and coverage. At present, the Internet has covered all aspects of people's lives, which facilitates people's life and work. However, due to the openness of the network itself, network security problems have followed. If these problems cannot be effectively solved, people's privacy security will be seriously endangered. Big data mining technology is one of the effective means to solve this kind of network security problems. We can find high-security and high-value information from a large amount of data, create a safe network environment for people, and provide great help for the subsequent development of computer networks.

Keywords: Application; Data Mining Technology; Network Security

1. What is data mining technology

In fact, data mining technology is a technology to identify, detect, classify and collect massive and noisy data, and find the laws that are not easy to be discovered in these data. Data mining technology mainly consists of three parts-data expression, data law and data preparation. It realizes data mining through the design and application of data mining mode and data mining engine. First, it puts forward specific requirements for data mining engine and classifies and collects data according to this requirement. This operation can also be called data preprocessing. Then, the rules existing in the data are mined, and the data rules that are not easy to be intuitively reflected by people are extracted. These data are useful potential rules, which lays the foundation for the subsequent analysis of the data.

2. Network security status quo

Usually, the network threats faced by enterprises usually include webpage intrusion, data leakage, network extortion, distributed denial of service attacks, etc. Hackers use website vulnerabilities to invade websites, and implant viruses to tamper with the contents of web pages, which has a negative impact on the normal development of enterprises. What's more, it will steal a large number of customer data accumulated by enterprises in production and operation, infringe on the privacy of others to extort money, and cause great economic losses to enterprises. The website will be attacked from multiple sites at the same time, which will flood the website server with a lot of information that requires reply, consume network bandwidth or system resources, and lead to the overload of the network or system and even paralysis, and stop providing normal network services.

International cyber attacks are more frequent. First, frequent security loopholes in software and hardware equipment pose a serious threat to production and life. Second, key information infrastructures in many industries are attacked. Third, personal information and business data are exposed and illegally used on a large scale. People's lives are inseparable from the Internet, and people's dependence on the Internet is greatly enhanced. Once network security is threatened, it will affect all aspects of people's lives and privacy will be endangered.

3. Data mining technology in the network security application process

Due to the complex process and large amount of data in the application process of data mining technology, it is necessary to clearly grasp the characteristics of each link and make reasonable plans for it in order to ensure the security of network application. Specifically, by constructing the following five analysis modules.

The first is the data source module, which can intercept the data sent or received through the network, dump the data, then process and edit the original data packet, and finally send it to the preprocessing module for further operation. Secondly, the preprocessing module, under which the data packet will undergo a series of operations such as feature standardization, change numerical mapping and original data standardization. After these operations, the original data packet is transformed, which improves the authenticity and accuracy of the data and meets various types of preprocessing requirements. The changed data packet greatly improves the efficiency and convenience of subsequent data mining operations, which is an extremely important step in the whole data mining technology. The third is the data mining module, which includes case-based reasoning, statistical methods, decision trees, fuzzy sets, genetic algorithms and other information processing methods. The information in the database is effectively analyzed and processed by this module, and the completed information is sent to the decision-making module. The fourth is the rule module, the main function of which is to record the characteristics of network security problems related to malicious attacks, abnormal intrusions and network viruses, and then provide theoretical support for subsequent network security protection with complete summary and classification. The fifth is the decision-making module, which can effectively match the data mining module and the rule base module. That is to say, if there is high matching data between the rule base module and the database mining module, it can be considered that the computer network security has suffered external threats.

4. Application mechanism of data mining technology

The application mechanism mainly discusses the functions of data collection, data processing, network security, database and data preprocessing.

4.1 Data collection

Under the background of information explosion, the network has penetrated into every aspect of people's lives, and people's personal privacy has been greatly threatened because of the development of the network. However, it is impossible for people to leave the information network in today's society. In this situation, higher requirements are put forward for network security, which requires protecting people's privacy in network security and using data mining technology to find hidden dangers in network security. Take network viruses as an example. Viruses are usually implanted into computers in the form of codes, and then penetrate the whole network. They will hide themselves and pretend to be other software, which makes it difficult to find out, and then destroy computer systems and leak network data and information. Big data mining technology is the key method to solve this kind of problems. Data mining technology can analyze a large number of data, find suspicious codes and analyze them, and clarify the key points in the codes, so as to find problems and solve them in time. Generally, network virus programs are similar to other software programs in computers, which are easily overlooked. Therefore, using data mining technology to collect virus code information can provide reliable data support for building a network security protection mechanism after classifying their common characteristics.

4.2 Data processing

In order to transform and crack all kinds of network program codes, the program codes should be converted into easily recognizable contents to ensure the timeliness and effectiveness of protection. By using its data processing module, network security problems can be identified and transformed, and then the address, ip address and specific information of data sources can be found out, and the address where ip is located can be accurately located, and the source of network security intrusion can be found out. After controlling the source of data, the transmission channel of data will also be blocked, so as to reduce the risk of the spread and diffusion of such network security problems and ensure that the harm of network security problems will be minimized. In addition, through big data mining technology, data information terminals can also be processed. By classifying, sorting and analyzing various data information, the analysis time and cracking efficiency of network security issues can be effectively improved, and the application of related data information becomes safer.

4.2.1 Network security

The application of data mining technology rule base module and data mining module can realize the matching of related data, and if the matching degree is high, the network security risks can be efficiently mined. At present, computer users will download all kinds of security protection software when facing many network security problems, such as Tencent housekeeper, tinder and 360 security guards, etc. Reasonable use of these software will play a great role in protecting computer network security and provide convenience for users. However, when users encounter various network security problems, these protection software will also have low recognition accuracy, unable to accurately judge network viruses and Trojans, and even delete some security programs by misjudging them as viruses. This is precisely because these protection softwares have yet to be perfected in the decision-making module, which leads to the lack of binding conditions for rule operation, and the application of big data mining technology can effectively solve the above problems.

5. The main application direction of data mining technology in network security

The detection forms of intrusion detection technology in network security protection mainly include two types: normal intrusion detection and abnormal intrusion detection, which are usually combined. The application of intrusion detection technology in data mining technology can improve the level of intrusion detection and the level of network security, and further improve the effect of network security maintenance.

5.1 Normal intrusion detection

Normal intrusion detection is to detect the object with normal network behavior, filter out the normal model characteristics through scientific and systematic analysis and modeling, and judge whether the user's network behavior is normal or not through the normal model characteristics and the user's network behavior characteristics. If the results do not match, it will be judged that the user's network behavior is abnormal intrusion. However, there is a certain error in judging this intrusion behavior from the technical level. Therefore, in the process of practical application of this technology, it is necessary to cooperate with the method of dividing the same type of data information to improve the accuracy of data analysis and ensure the accuracy of detection results.

5.2 Abnormal intrusion detection

Anomalous intrusion detection is mainly aimed at the detection of abnormal behaviors. First, it collects abnormal behavior data, constructs relevant models to analyze these abnormal data and further summarizes and analyzes these intrusion behavior characteristics, which makes the anomaly analysis model more comprehensive and rich. In this way, once the abnormal intrusion behavior of the knife is detected, the abnormal intrusion detection technology can detect the characteristics similar to the previous intrusion, and quickly identify and analyze the intrusion behavior. Compared with normal intrusion detection, the data information of abnormal intrusion detection is relatively simple, and the established model is relatively easy.

6. Conclusion

To sum up, the internet is an inseparable part of people's lives, which brings us great convenience and risks, and corporate information, personal privacy and confidential documents are all threatened by leakage. Therefore, it is particularly important to strengthen the defense system of network security and raise the awareness of network security prevention of the whole people. In solving this problem, the application of data mining technology has played a particularly important role, which has a very positive effect on the improvement of computer network security. Therefore, web workers needs to attach importance to the role of data mining technology and apply it reasonably in combination with the actual situation, so that it can play a more critical role in the protection of network security issues.

References

[1] Jiang YP, Application of Data Mining Technology in Network Security [J], Information Systems Engineering, 2023 (05), 73-75.

[2] Xu H, Application of Data Mining Technology in Computer Network Security [J], Integrated Circuit Applications, 2023 (05), 92-93.

[3] An SY, Data Mining Technology and Its Application in Network Security [J], Computer Knowledge and Technology, 2019 (04), 10-11.

[4] Wu YN, Application and Research of Big Data Mining Technology in Network Security [J], Network Security Technology and Application, 2022 (07), 55-56.