Analysis on the Application of Data Mining in Network Security

Zhi Liping, Zhu Shuaibo

School of Computer and Information Engineering, Anyang Normal University, Anyang, China
Correspondence: Zhi Liping, School of Computer and Information Engineering, Anyang Normal University, Anyang, China

Abstract: The development of network technology has greatly promoted the progress of society. It is in recent years that Internet technology has been popularized in China and has had a significant impact on people's work and life. It makes people more comfortable and faster to obtain information than before, and has become an important tool for people's office and entertainment. At the same time, some uncertain factors in the network are increasingly becoming a huge hidden danger threatening the society. In this context, we analyze the use of data mining technology to maintain network security.

Keywords: Data mining; Network security; intrusion detection

1. Introduction

In recent years, with the continuous improvement of database, data mining technology is developing gradually. In fact, data technology covers more fields than general fields. In the context of actual use, it is often integrated with AI technologies, artificial intelligence, large databases, machine learning and other technologies. From an economic point of view, data mining shows clear commercial value and is likely to be used in more fields in the future. However, data mining technology has not reached the mature state of use, data collection and research there are many security risks, especially network security and data privacy protection. To ensure the security of computer network is the premise of improving the influence of computer network use. In most fields, the use of computers more and more, network virus intrusion network security speed "development" has been constantly improving, so there are more and more network security problems, causing a great threat to the security of the computer network. The effective application of data mining technology will help alleviate the above problems.

2. Data mining technology

2.1 Concept of data mining

As a new business information processing technology, data mining in the United States began in the 1980s and was first applied in the fields of finance and telecommunications. At present, data mining is a hot issue in data science and artificial intelligence database. It has a wide range of applications. Its main advantages are the collection, processing, analysis, modeling, and visualization of large amounts of previously collected data and the extraction of key information useful for business decisions. It should be emphasized that the data itself has no value, but the information contained in the data as a carrier has commercial value and high investigation value. The so-called data extraction technology refers to the direct and indirect disclosure of massive data. The basis of decision support is data mining, which is mainly based on AI intelligence, automatic learning, statistics and other technological technologies. It can automatically and independently analyze a large amount of data of the enterprise, draw abnormal logic from the massive data, so as to establish an effective model to help relevant decision makers adjust strategies, reduce risks, and make the right decision.

2.2 The role of data mining technology

Over the years, with the rapid development of 5G communications, artificial intelligence, Internet of Things, blockchain and other technologies, information has exploded, and a large amount of data contributes to people's life and work. It can be said to be an important factor in promoting current social progress. At the same time, a large amount of information, such as invalid and negative information, is also huge, without review and selection, and has a certain impact on social progress, or even has the opposite effect. How to find truly meaningful and positive information data from the mass of information, in order to meet the needs of various users, various scenarios and various fields, the application of big data mining technology is very important and necessary. With the development of society and the continuous improvement of science and technology, there are more and more network equipment with various performance. To realize high-speed transmission of information data, it is more important to collect information data. In recent years, with the development of traditional technology, organized database is the main processing method for storing information. Not only is the cost high, but there is also the problem of data loss. Effective application of big data mining technology can reduce the possibility of data loss, improve work efficiency, thus ensuring the accuracy and efficiency of data collection, processing and use. At the same time, it also plays an important role in the application of data mining technology to effectively improve network security defense system.

3. Common problems in network security

3.1 Means by which criminals maliciously destroy networks

3.1.1 Hacker Attacks

Hacker attack is the most common network security problem. The attack may make the network channel inaccessible or lead to the interception and eavesdropping of important information and data. The so-called hacker attack is the malicious destruction of network information. This behavior has obvious destructive color, hackers are usually very cunning when attacking the target of invasion, they usually will first invade the computer, and then tamper with and destroy the programming software, rather than directly invade important elements, usually can be divided into active attack and passive attack. The target of an active attack is usually specific in order to gain some information or damage some object. Most of this hacking is illegal and can render online information unusable. For example, some small game developers in China are often attacked by foreign criminals, and their protection ability is relatively weak. Through a number of persistent attacks, users were unable to access the game operators' servers in order to extort money. Passive attacks do not affect the normal use of the network, but hinder the network connectivity, which is also a serious threat.

3.1.2 Computer virus attacks

When a computer program gets a virus, it can be difficult for a computer owner to detect it in time, and often only when something goes wrong does the computer realize it's a virus. Compared with individuals, enterprise computer virus intrusion is more harmful. If a company's computers are invaded by a virus, not only are they unusable, but some important data may be stolen. So, do a good job of computer virus protection is the most important.

3.2 Harm of network crime

Bank card theft, telecom fraud and other cyber crimes have been reported in alarming numbers in recent years. Generally speaking, the main threat of cyber crime is mainly manifested in two aspects.

3.2.1 Result in the disclosure of citizenship information and state secrets

At present, criminals illegally steal confidential information through hackers or computer viruses, thus revealing state secrets and citizens' information, endangering national security, social stability and people's lives and property.

3.2.2 Endanger people's financial security

Online trading platforms such as Alipay and third-party clearing and trading have become popular in recent years. However, there are also some loopholes in the regulatory measures, which provide opportunities for criminals to steal money illegally and carry out financial fraud through the Internet, seriously endangering people's financial security.

3.3 Shortcomings of traditional network intrusion detection methods

Network intrusion detection is an important measure to maintain network security. There are mainly two effective methods: the first is abnormal intrusion detection, the second is misuse intrusion detection. Although up to now network intrusion detection technology has made great progress, but generally speaking there are still some shortcomings.

3.3.1 Disadvantages of misuse of intrusion detection methods

If the network intrusion detection method is not used correctly, it will lead to failure to find new intrusion behaviors. Of course, its detection results will not have practical significance, so it is seldom used in network intrusion detection at present.

3.3.2 Disadvantages of abnormal intrusion detection methods

Network intrusion detection methods mainly include Bayesian network, neural network, statistical method and data mining. Compared with the illegitimate intrusion detection method, this obviously greatly improves the detection effect, but there are still some disadvantages. Among them, anomaly intrusion detection based on statistics is the most basic method, it can only be used for some small network detection, there is no way to achieve large-scale network detection. Compared with the bayesian network and neural network, the detection rate is high, but the false alarm rate is high, and its adaptability is insufficient. And in the face of the rapid development of high-tech network intrusion means, this method is becoming more and more difficult.

4. The application mechanism of data mining technology in network security

4.1 Application of data mining technology in data acquisition

In the information age, the rapid growth of data information, especially the increase of data privacy, this phenomenon has put forward higher requirements for network security. An important factor in data leakage and corruption is virus code. The main method of data mining technology is to collect data information, and timely and effective discovery of some vulnerabilities in network security, the virus code and data information security risks of the virus mining, quickly and effectively prevent abnormal intrusion and tracking and a series of problems. Usually, network viruses invade the computer system step by step, and finally they destroy the entire computer system with the help of computer programs. Data mining technology can make a comprehensive analysis of all kinds of code programs, dig out the key points of code programs, quickly find out the problems existing in different programs, and take effective preventive measures. Some computer programs are very similar to network viruses, which are particularly difficult to detect and easy to miss, leading to the failure of the computer system. Therefore, it is necessary to collect network virus code and program information through big data mining technology, and classify it according to its incidence, so as to provide certain information support for establishing network security protection mechanism.

4.2 Application of data mining technology in data processing

Data mining technology can analyze and process data and information according to the deep information in data mining, so as to discover and identify the root of network security problems scientifically and effectively. Under normal circumstances, network security problems can be compromised by program code. Therefore, it is necessary to modify and disassemble network program code, so that technicians can identify and disassemble the basic intent of program code, so as to achieve the purpose of protection. In order to transform and decode the program, it must be done through the data processing module, which can identify the data source, IP and other basic information. Then a comprehensive root extraction is carried out to locate the target IP address and lock the root of the network virus. In order to prevent the spread of network viruses, we try to control the limited range of network virus attacks and avoid the further spread of viruses. At the same time, large-scale data mining technology can also analyze, classify and process data and information terminals. On the basis of data processing, it greatly improves the efficiency of solving network security problems and provides an important guarantee for network information security.

4.3 Application of data mining technology in database

The application of database is mainly to analyze the association of database, an application to analyze the relationship between databases, which provides the search basis for the clustering of data technology. This foundation, combined with network security issues, provides in-depth identification. When a virus logs on to a network program, the attack path is logged using the associated database to perform the attack level. Then, the clustering analysis method is used to identify the characteristics of network viruses to improve the overall protection ability of computer systems.

4.4 Application of data mining technology in decision-making mechanism

The data mining module has the function of data analysis and memory, which is compared with the rule-based module. If there is a high degree of data match between the two, it means there is a network security risk in the computer system. Firewall 360 is commonly used in computer systems. However, 360 firewall's evaluation accuracy of virus network attributes is not high, there are evaluation errors, network security decision-making mechanism is not ideal. Therefore, data extraction techniques should be used to interact with the decision module. It is necessary to increase scientific and effective decision making according to the characteristics of viruses in the network, so as to avoid undue interference to data due to inadequate system judgment, and even provide the possibility of heredity for virus programs.

4.5 Application of data mining technology in data preprocessing

Data preprocessing is the process of analyzing, classifying and modifying viruses according to their characteristics and decision-making needs. The goal is to improve data processing results. The purpose of data preprocessing scheme is to scientifically verify the security of network information, allocate key data parameters and validation indexes, and provide important basis for national defense system construction. Therefore, in the application of data acquisition technology, the data can be accurately analyzed and processed, and the original characteristics such as virus type and system vulnerability can be assessed, so as to improve the defense ability of computer system to a certain extent.

5. Application direction of data mining technology in network security

In order to ensure network security, intrusion detection technology is one of its key modules. At present, there are two methods to detect intrusion: common intrusion detection and abnormal intrusion detection. They are different, but they are often used together. Using data acquisition technology to detect network security vulnerabilities can significantly improve the technical level of intrusion detection, so as to maintain a higher level of network security.

To discover abnormal intrusion, the most important thing is to collect abnormal data and establish a scientific and effective model. At the same time, the characteristics of intrusion behavior should be analyzed and summarized to enrich the anomaly data model. So if an illegal intrusion occurs again, the detection technology will pick up signs similar to the previous abnormal intrusion and will quickly stop the virus from entering and spreading. The identification information of intrusion data is relatively simple, and the data model is also easy to create. However, this intrusion detection technology can only judge the previous abnormal intrusion behavior, but can not accurately identify the early or undisturbed intrusion function, and has many weaknesses. The use of large-scale data mining technology can help the intrusion detection technology determine the function of predicting intrusion behavior without knowledge. Its main principle is to analyze and extract historical data through intrusion data communication technology, then dig and analyze intrusion path, create data classification parameter pattern, and predict intrusion through arithmetic science. The combination of intrusion detection technology and data mining technology makes great contribution to the prediction and analysis function of data mining technology. It can predict and detect abnormal intrusion detection timely and effectively, and improve the accuracy of intrusion detection.

Different from the normal intrusion detection, the normal object of intrusion detection is the normal network behavior, which should be scientifically and systematically analyzed and modeled, and the normal characteristics of the model should be removed. By comparing the correspondence between user behavior characteristics and normal model characteristics, we can determine whether the network behavior is normal. If the user behavior does not conform to the normal characteristics of the model, it is regarded as abnormal intrusion. In this way, you may make some mistakes. Therefore, the use of big data acquisition technology in traditional intrusion detection technology can classify data into the same category, improve the accuracy of data, improve the accuracy of intrusion detection.

6. Conclusion

With the advent of the network era, network applications permeate into every aspect of people's life. It not only brings convenience to people's life and work, but also affects information security. Therefore, it is particularly important to strengthen network security management. The application of data mining technology to network security can give full play to the advantages of large-scale data mining technology, improve the anti-virus ability of network system obviously, and avoid the network system virus invasion program. Therefore, we should strengthen the research and application of data mining technology, improve the network security management environment, and promote the development of a healthier network environment.

References

[1]. Dong Xinge. Analysis on the application of data mining technology in banks under the background of big data [J]. Today's Wealth, 2021(20):31-33.

[2]. Qiu Jinlong. Application of big data mining technology in network security [J]. Electronic Technology and Software Engineering, 2021(12):259-260.

[3]. XIONG Yi. Research on application of Big data Mining technology in network security [J]. Paper Equipment & Materials, 201, 50(02):104-105+111.

[4]. Chen Jie. Application analysis of Data Mining technology in Network Security [J]. Network Security Technology and Application, 2020(12):63-64.

[5]. Liu J. Application of data mining in computer network security [J]. Digital World, 2017(11):49. (in Chinese)

[6]. LIANG Yu. Research on application of data Mining technology in network intrusion Detection [J]. Computer Programming Skills and Maintenance, 2014 (22): 93-94.