Talking about the Application and Development of Data Mining in the Field of Computer Network Security

Yong He¹,*

¹School of Preschool Education, Jiangxi Teachers College, Yingtan, 335000, China

*Corresponding author: hy15731555@jxsfgz.com

Abstract. While computers bring great convenience to people, they also bring a lot of risks. Some illegal elements use network viruses to invade users' computers and steal data, which causes users' information to leak. Therefore, we must establish a secure virus defense system, which can protect users' information security and resist virus intrusion.

Keywords: Computer Network, Virus Defense System, Security Field, Data Mining

1. Introduction

With the advent of the information age, while bringing convenience to people, it also makes people increasingly dependent on computer networks. Now society only needs a computer to complete most of the work, but computer network has the characteristics of openness and sharing, this greatly affects the security of data information. Applying data mining technology can solve this problem effectively. This technology can extract concealed related information, it has great application value in the field of computer network security [1].

2. Data mining technology

Data mining refers to the non-trivial process of revealing hidden, previously unknown and potentially valuable information from a large amount of data in the database. Data mining is a decision support process, which is mainly based on artificial intelligence, machine learning, pattern recognition, statistics, databases, visualization technology, etc., highly automated analysis of enterprise data, making inductive reasoning, and digging out potential patterns from it, it can help decision-makers adjust market strategies, reduce risks, and make correct decisions.

3. Application of data mining technology

3.1. Possibility for use in network virus defense system
In order to apply data mining technology better, we need understand and analyze the propagation process of network viruses and provide a basis for the application of data mining. If a worm virus infects a computer, you first need to scan the hosts on the network. This process is the key to detecting worms, and it is also a breakthrough point in building a computer prevention system [2]. The new network virus defense system is composed of data source modules, preprocessing modules, data mining modules, rule base modules, decision-making modules and defense modules. Its working principle is: After the data packets from the network and sent to the local form the data source, they are processed by the preprocessing module, and the virus transmitted by the network information is recorded, so as to form immunity to the virus of the same nature in the later period. Once these viruses invade illegally again, the system will promptly alert and activate the corresponding protection and defense programs. Figure 1 is a schematic diagram of the data mining structure [3].

![Schematic diagram of data mining structure](image)

**Figure 1.** Schematic diagram of data mining structure

### 3.2. Application in the construction of network virus defense system

The new computer network virus defense method can deal with computer network information security issues more comprehensively and effectively. Specifically, we can analyze its application in the process of computer network virus defense from the following perspectives:

① Data source module. This module is based on the packet capture program to intercept the data packet information sent by the network to the host. The data source module has the most primitive data packet and data structure. After obtaining such a data source, it must be handed over to the preprocessing module for the next step [4].
② Data preprocessing module. This is the basic work of data mining technology, and this work will lay a good foundation for later data analysis. It is not only related to the effectiveness of data mining, but also related to data mining time.

③ The rule base module. Its efficiency is mainly to store the detected virus characteristics and accumulate them to form a rule set. This point reflects the characteristics of the virus and the rules for connecting data, and provides a corresponding basis for later analysis and collection of virus data characteristics.

④ Data mining module. Analyze the event library with the help of scientific algorithms, and generate request records on this basis, and hand it over to the decision-making module after completing this work.

⑤ Decision module. The effectiveness of this module is to analyze the matching degree between the results of data mining and the rules of the rule base. If it is found that the match between the two is relatively high, it means that there may be a virus in the data packet; if the match between the two is found to be very low, an early warning mechanism can be launched on this basis to find a new worm, and incorporate it into the rule base to realize the expansion of the rule base [5].

3.3. Decision tree mining

A decision tree is actually a tree-like graph, which is mainly composed of multiple nodes. Each node has a separate property test. The branches represent the detection results, and the leaf nodes represent different forms of state distribution. On the classification tree, the most basic algorithms are ID3 and C4.5, and the method is mainly a top-to-bottom structure. The specific process of decision tree mining is shown in Figure 2.

![Decision Tree Diagram](image)

**Figure 2.** Decision tree mining process

The specific description is the decision-making conditions for malicious viruses. First, malicious programs have the ability to destroy, second, malicious programs have the ability to infect, and third, malicious programs have the ability to hide. The main job of the computer network security virus defense system is to grab samples in time to help users develop solutions. The decision tree model can greatly...
reduce the tasks that require manual sorting in traditional virus defense projects, and prompt relevant employees to analyze virus-like samples first, thereby improving the efficiency of analysis and processing [6,7].

4. Strategies for building a network virus defense system

Theoretical research is the prerequisite of data mining technology and the driving force for software companies to promote data mining technology. The construction of a standard system is the focus of a stable operating environment, and application talents in data mining technology are a key factor in advancing various tasks. Obviously, the above content is to construct a computer network virus defense system from a technical point of view. But in actual situations, if we want to give full play to the role of this technology in computer virus defense, we must also do the following tasks.

4.1. Attach great importance to the theoretical research of data mining technology

Technical theory research is the basis and prerequisite for exerting practical application efficiency. In order to better realize the application of this technology, we should work hard to do the following three aspects: ① We should pay attention to the theoretical research of this technology, encourage scholars and experts to study this content, and learn from the advanced technology of Western countries. Constantly improve the theoretical system with theory; ② Pay attention to the exchanges between academia and the industry, advocate integrating theory with practice, forming a virtuous circle of theory guiding practice, and promoting theory with practice, and on this basis, realize the overall development of the theoretical system of data mining technology; ③ Active research The relationship between data mining technology and computer network virus defense, and on this basis, a network virus defense system is developed and designed [8].

4.2. Encourage the healthy development of domestic software manufacturers

The research system of data mining technology in foreign software companies is relatively mature and can be applied to actual production. There are not many similar software companies in my country, and the research and development in this area is still in its infancy. Therefore, we need to actively encourage the development of domestic software manufacturers and build a relatively healthy market environment for them. Of course, such software manufacturers should continue to learn and research foreign advanced technology, and apply this technology to the field of computer network virus defense. In addition, domestic software manufacturers should establish a sound industry communication mechanism to summarize the application experience of this technology in computer network virus defense, which will help promote the development and progress of the industry.

4.3. Focus on training professional network management talents

Similar to the formalization and standardization of the SQL language, data mining technology will develop in the direction of standardization. If it is applied to the relevant data language system, the quality of data mining can be continuously improved, so that customers can better understand the intention of the other party, thereby achieving more efficient human-computer interaction effects, and handling the relationship between the mining technology server and the database server. Give full play to its effectiveness in unstructured data. In the process of establishing the data mining technology
standard system, we should always adhere to the market demand-oriented and specific analysis of specific issues to meet the market's demand for mining technology [9].

4.4. Establish and improve the standard system of data mining technology

In the final analysis, the purpose of applying database technology to the computer network virus defense system is to maintain the security and stability of the network, so that good business transactions can be achieved in the network environment. But no matter what kind of operation, we all need professionals to complete this series of operations, otherwise there will be many loopholes in the system. In view of this, it is necessary to attach great importance to the training of professional talents. On the one hand, it is necessary to actively contact universities and use data mining technology as the course content to cultivate professional network security management talents; On the other hand, it is necessary to focus on the development of professional training within the enterprise [10]. We should improve the skill quality of professionals and ensure the effective operation of the computer network virus defense system.

5. Conclusion

In summary, computer network security viruses directly threaten the security and stability of users and enterprises. It will directly lead to disclose personal information and commercial secrets, which will cause irreparable huge losses. This requires relevant departments to improve the computer network security virus defense system. We must rationally apply data mining technology and improve the stability and effectiveness of the virus defense system. This will protect personal and corporate information from infringement.

References

[1] LIU Ji. Application of Data Mining in the Field of Computer Network Security [J]. Digital World, 2017:49.

[2] LI Liangchao. Application of Data Mining in Computer Network Security [J]. Science and Technology Innovation, 2015:115-116.

[3] ZHANG Yan. Application of Data Mining in the Field of Computer Network Security [J]. Computer Disc Software and Application, 2014:170-171.

[4] GAN Yi-jun. Application Analysis of Data Mining in the Field of Computer Network Security [J]. China New Communications, 2018:159.

[5] LIU Xin. Application Value of Data Mining in the Field of Computer Network Security [J]. Journal of Liaoning Radio and TV University, 2017.

[6] He Guangning. Research on Application of Data Mining in the Field of Computer Network Security [J]. Technology and Market, 2016:13-13, 15, 2 pages.

[7] CHEN Lei. Discussion on the Application of Data Encryption Technology in the Field of Computer Network Security [J]. Netizen World, 2013:7. LI Jia-jia. Application of Data Mining in Computer Network Virus Defense [J]. Network Security Technology and Application, 2017.
[8] ZHANG Yu. Discussion on the hidden dangers of computer network security and the application of data encryption technology [J]. Computer CD Software and Application, 2013: 180+182.

[9] Qing-yi liu;. Application of Data Mining Technology in Computer Network Security Virus Defense [J]. Microcomputer Application, 2018: 76-78.

[10] Li Jiajia. On the application of data mining in computer network virus defense [J]. Network Security Technology and Application, 2017.