IOP Conf. Series: Materials Science and Engineering **382** (2018) 052019 doi:10.1088/1757-899X/382/5/052019

Computer Network Virus Defense Technology Based on Data Mining Technology

Author's name：Hui Yin

Author unit：Shandong Judicial Police Vocational College

postal code：250014

Abstract: The expansion of the application scope of computer networks in the current situation has brought important guarantee of the continuous improvement in the production level of China's information industry. In this context, in order to achieve the safe use of computer network, making it practical to effectively deal with the virus, you need to strengthen the use of the virus defense technology associated with it, enrich the computer network virus defense technology content, enhance the applicability of the technology in the data mining technology. Therefore, this article discusses the technology of computer network virus defense based on data mining.

1. Introduction

Pay attention to data mining technology-based computer network virus defense technology analysis and use is conducive to efficient computer network virus processing, giving users the scientific information security in order to promote the practical application of computer networks which can be stable and efficient operation. Therefore, we need to combine the actual requirements of computer network virus processing and the functional characteristics of its defense technology to give more attention to data mining technology, and apply the technology to computer network virus defense technology, making the potential application value of such defense technology to upgraded to meet the actual needs of computer network security to the maximum.

2. Features of Computer Network Virus in Practice

If there is a virus in the practical application of computer network, the security of the computer network will be threatened potentially, which indirectly increases the risk of computer network operation, which may result in the occurrence of user data loss and information leakage. In response to this situation, in order to improve the correct understanding of computer network viruses, to provide the necessary reference for the rational choice and use of its defense technology, you need to strengthen the characteristics of computer network virus. These features are manifested in the following aspects:

2.1Diversity of Forms of Communication

Due to the existence of loopholes such as e-mail, system and bad webpage in the practice of computer network, the network virus can spread through these channels, which brings some damage to the computer network and makes the security in operation lack of reliability protection. In practice, due to the computer network virus program code can be scanned on the host system, search and scan folders, making the diversity of the form of communication is characterized by significant. Therefore, when

analyzing computer network viruses, it is necessary to fully consider the impact caused by the diversity of their forms of transmission, so as to provide reference information about the application of the necessary defensive techniques [1].

2.2 Variety of Species

Computer network virus plays an important role in the process of practice, We can use the advantages of using code, form a wide range of network viruses, and make the appropriate changes. On this basis, the network virus will have a greater impact on the operation of the computer network, and as its reproduction speed and type of increase, making the computer network security is not optimistic. Therefore, in the implementation of computer network virus defense technology research process, we need in-depth analysis of the diversity of their species, so that the computer network virus defense technology is more scientific to maintain its practice of good virus defense effect.

2.3 Practical Pertinence

Under the current situation, with the development of the computer network and the continuous improvement of its technical level of virus design and development, it is possible to carry out targeted destruction in the course of network virus practice and make the computer network virus defense technology more difficult. At the same time, if the computer network virus design and development mode to support and accelerate its development in the direction of commercialization, it will make it more harmful to the targeted implementation of the destruction of operational behavior, we need to be based on data mining technology of computer network virus defense technology support in order to achieve the scientific treatment of network viruses [2].

3. An Overview of Data Mining Techniques and Analysis of Main Methods in Practice

3.1Practical Data Mining Technology Overview

Data mining technology is through all the data onto a certain range of data collection, data classification and data collection, and then determine whether there is a potential relationship between the law and data, there are three main areas: The first is prepare data ; the second is to find the law of the existence of data ; the third is to show the law of data. Through in-depth analysis of the data processing status of these different links between the practice, it is helpful to optimize the application structure of data mining technology so that the potential application value of the technology can be improved, thus providing the necessary technical support for the use of computer network virus defense technology.

If you need to take advantage of data mining technology to deal with network viruses in the application of computer network virus defense technology, you need to pay attention to the effective setting of data mining mode, combined with the database's functional characteristics and requirements, the data to be processed scientifically class, to determine the relationship between different data, to master the laws between the data, so as to provide follow-up data processing work to provide reference information. At the same time, due to the many operation steps involved in the application of data mining technology and the complicated working process, relevant personnel are required to implement the corresponding work in the preprocessing stage during the data mining application, so that the data purification and format conversion, variable integration and so on to maintain good effect, and then play the advantages of data mining technology to meet the technical requirements of computer network virus defense [3]. The structure of data mining technology in practice is shown in Figure 1.

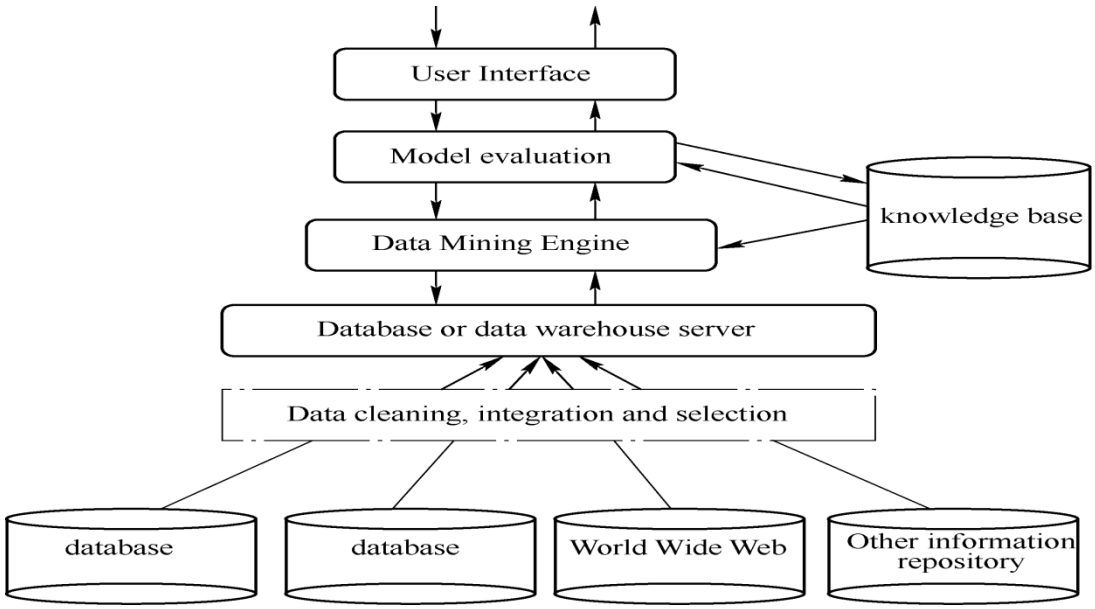

Figure 1 the structure diagramin the practice of data mining technology

3.2 Analysis of Main Methods of Data Mining in Practice

3.2.1 Actual Statistical Method

With the advantage of statistical methods in data mining, it can provide a guarantee for enhancing its practical application effect, and gradually increase the potential application value of data mining technology, and play a due role in the application of computer network virus defense. In practice, through the association and function of the establishment of two relations we can achieve the effective setting of the field of the database items. At the same time, through the efficient use of different statistical methods, such as regression analysis and principal component analysis, data mining can be given the necessary support.

3.2.2 Decision Tree in Practice

In the process of data mining, if the data needs to be scientifically classified, it can be dealt with under the action of the decision tree. Decision tree-based data classification projects include: through the rational use of existing data to achieve the decision tree in order to create ; in the process of sound decision tree, the gradual realization of scientific data prediction. In the meantime, if we can get a correct understanding of the law of data generation, we can provide the necessary reference information about the establishment of the decision tree to meet the requirements of the visual data rules for the maximum, so as to deepen the data mining process and output results understanding. In practice, the decision trees can maintain good accuracy under the condition of effective information and the high efficiency in the application makes them occupy an important position in the data mining method. Therefore, in the application of data mining methods, the decision tree should be strengthened [4].

3.2.3 Mining Association Rules in Practice

The so-called association rules, refers to the application of the database contained in the association with objects rules. In the process of application, the advantages of correlation analysis can be used to find out the hidden relations needed, so as to provide a reference to the processing of unknown problems, so that the data mining method can achieve the desired results from application and meet the actual requirements of computer network virus defense. For example, in practice, if the support degree of a non-empty item set is known (as shown in Table 1), and the association rules whose

reliability are greater than 95% are valid, determine the corresponding reliability rules in the table. The specific analysis process is as follows:

Table 1 a non-empty itemset support in practice

Non-empty item set	Support	Non-empty item set	Support
{x,z}	60%	{x}	100%
{y,z}	35%	{y}	70%
{x,y,z}	35%	{z}	60%
{x，y}	70%		

Combined with the contents described in Table 1, the following aspects can be analyzed when determining the number of valid non-empty itemsets association rules:

{X} → {y} confidence ({x} → {y}) = support ({x, y}) / support ({x}) = 70% / 100% = 70%

{Y} → {x} confidence ({y} → {x}) = support ({x, y}) / support ({y}) = 70% / 70% = 100%

{X} → {z} confidence ({x} → {z}) = support ({x, z}) / support

{Z} → {x} Credibility ({z} → {x}) = Support ({x, z}) / Support ({z}) = 60% / 60% = 100%

Through in-depth analysis of the above rules in practice, it can be known that {y} → {x} and {z} → {x} are valid associated reliability rules that are greater than 95%, there are two list.

4. Analysis of Computer Network Virus Defense Technology Based on Data Mining Technology

4.1 Data Mining Technology Analysis of Different Modules

In the defense of computer network viruses, the use of data mining based on network virus defense technology need to deal with the need for the technology involved in the analysis of the different modules. These modules include the following:

4.1.1 Data Preprocessing Module

Simplified data mining technology in the data mining and data processing between the operation can be achieved through the data preprocessing module to achieve the use of data preprocessing module which can improve the overall data mining results and improve data identification and accuracy. After completing the data collection, the data needs to be imported into the preprocessing module to realize the data classification and data transformation, and in this way, the data can be converted into the data content that can be identified and processed by the system. In practice, through the reasonable setting and use of this module, the data can be efficiently processed [5].

4.1.2 Decision Making Module

With the support of this module, data mining can be constructed and matched with the data in the database to determine whether there is any characteristic of network virus in the decision module so as to improve the reference for timely processing of computer network virus.

4.1.3 Data Collection Module

In order to realize the effective use of data mining technology in computer network virus defense, it is

necessary to pay attention to the full utilization of data information. Therefore, it is necessary to capture and collect the information contained in the data packet of the computer network with the support of the data collection module, and to provide the required information for the data mining process while meeting the actual needs of computer network virus defense [6].

4.1.4 Data Mining Module

When using data mining technology for computer network virus defense processing, data mining module should be set up when data generated in the operation of computer network needs to be processed with the support of event library and data mining algorithm. Under the function of the module, the data onto the event library can be effectively sorted and scientifically classified, and the required data structure can be obtained to effectively defend the network virus.

4.1.5 Rule Base Module

Through the effective setting of the module, the data analysis and identification in the computer network can be realized, so that the computer network virus can be processed timely in the data mining process and the network virus properties can be recorded to ensure the processing effect of the potential computer network virus is good [7].

4.2 Analysis of Computer Network Virus Defense System Based on Data Mining Technology

In the data mining technology support, computer network virus effective defense, should pay attention to powerful network virus defense system construction. The key points of its construction include: (1) The rational use of association rules. The association rule of data mining refers to the existence of knowledge that can be found in the same type of data. If two or more than two variables are selected, if the data is found to have a certain regularity, the data between the data and number. There is some kind of relevance. Emphasis on the rational use of association rules for data mining technology is conducive to improve the computer network virus defense system service functions ; (2) Emphasis on cluster analysis. Through cluster analysis in data mining technology, the corresponding computer network virus defense system is constructed, which is conducive to real-time analysis of the network virus distribution and to deal with it ; (3) To strengthen the classification analysis. When using the data mining technology to build a computer network virus defense system, if we can strengthen the classification analysis, we can achieve the data classification models construction, and improve the efficiency of network virus processing in the system operation [8].

5. Conclusion

To sum up, strengthening the use of computer network virus defense technology based on data mining technology has important practical reference significance: it is beneficial to enhance the practical application effect of the defense technology required in the computer network virus processing, and the computer network security status can be improved. In order to meet the actual needs of users to the maximum extent, making our computer network virus defense technology to enhance the level. Therefore, in the future, in the process of implementing computer network virus defense technology research, more attention should be paid to data mining technology with good applicability, so that the processing efficiency of computer network virus can be continuously improved, and thus the sustainable development of China's information industry lay a solid foundation.

References:

[1] Sun He. Analysis of data mining technology in computer network virus defense [J]. Jilin Labor Protection, 2016, (11).
[2] Zhang Yan. Application of Data Mining Technology in Computer Network Virus Defense [J]. Journal of Taiyuan Urban Vocational College, 2016, (04).
[3] Zheng Gang.Application of data mining technology in computer network virus defense [J].Journal of Information and Computer (Theory), 2016 (03).

[4] Liang Xue-Ting. Research on Computer Network Virus Defense Technology of Data Mining [J]. Science and Technology Economic Market, 2016, (01).
[5] Tang Ying.Application of Data Mining Technology in Computer Network Virus Defense [J].Journal of Information and Computers (Theory), 2015, (21).
[6] Chen Ding.Data Mining Technology Analysis of Computer Network Virus Defense Technology [J]. Electronic Technology and Software Engineering, 2015 (18): 207-208.
[7] Chen Chun. Computer network virus defense based on data mining [J]. Information & Communications, 2015 (, 05).
[8] Liu Chunjuan.Application analysis of data mining technology in computer network virus defense [J].Electronic Testing, 2014, (05).