Hindawi
Security and Communication Networks
Volume 2023, Article ID 9840486, 1 page
https://doi.org/10.1155/2023/9840486

Retraction

Retracted: Application of Data Mining in Predictive Analysis of Network Security Model

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Bian and S. Fu, "Application of Data Mining in Predictive Analysis of Network Security Model," *Security and Communication Networks*, vol. 2022, Article ID 4922377, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4922377, 8 pages
https://doi.org/10.1155/2022/4922377

Research Article

Application of Data Mining in Predictive Analysis of Network Security Model

Jinliang Bian and Shuguang Fu

Qingdao Vocational and Technical College of Hotel Management, Shandong, Qingdao 266100, China

Correspondence should be addressed to Jinliang Bian; 201704428@stu.ncwu.edu.cn

Received 24 April 2022; Revised 8 June 2022; Accepted 30 June 2022; Published 15 July 2022

Academic Editor: Mukesh Soni

In order to improve the application effect of data mining in the predictive analysis of network security models, this paper starts with the concept of data mining and data sources, then introduces related technologies from data mining technology and security setting collection technology, and finally introduces the computer network security maintenance system based on data mining. The results show that data mining technology plays an important role in the predictive analysis of network security models. The data show that by the end of 2021, the number of security vulnerabilities collected by my country's information security vulnerability sharing platform has reached 14,871, an increase of 46.6% compared with 2020. Among them, there are 5,567 high-risk vulnerabilities, an increase of about 1,400 vulnerabilities compared with last year. It can be seen that the number of vulnerabilities discovered every year and the number of high-risk vulnerabilities are basically increasing year by year. Therefore, it is recommended to strengthen the promotion of data mining technology in the predictive analysis of network security models, so that it can play a greater role.

1. Introduction

As the information technology of the network continues to evolve, people's work, life, entertainment, and other things are inextricably linked to the network. Although the Internet has brought a lot of convenience to people, it has also caused some network security problems, even information leakage, tampering, theft, and property loss caused by information security problems [1, 2]. Therefore, it is necessary to strengthen the security of the network. As the network technology develops, the factors that threaten the security of the network are increasing and seriously affect the privacy and security of the Internet citizens. Improving the safe use coefficient of Internet network is the so-called goal of public expectation. This article discusses strategies for using data mining technology for network security to improve the overall level of network security protection [3]. At present, the data mining algorithm has been successfully applied in sports, industrial production, people's daily life, transportation, and other different fields and has gradually begun to provide people with various personalized services, and its potential is being continuously explored. But in the computer network security maintenance, especially in the virus inspection and processing and other aspects, its application is relatively few.

In recent years, with the continuous improvement of large databases, data mining technology is also gradually developing. In fact, big data technology involves more disciplines than cross disciplines. In the real use background, it is often combined with AI technology, artificial intelligence, big database, machine learning, and other technologies. From the perspective of economics, data mining technology has shown the obvious commercial value and is likely to be applied to more fields in the future [4–6]. However, at present, data mining technology has not yet reached the state of mature use, and there are many security risks in the research of data adoption and use, especially network security and data privacy protection [7]. This paper examines the use of data mining technology in computer network security maintenance, strive to carry out various

services for computer network security maintenance, improve the maintenance level, ensure the maintenance quality, and contribute to information security. Figure 1 shows the use of data mining technology for network security. Among the many key technologies, data mining technology is one of the most important technologies. Data mining technology is to extract the data rules that are not easy to be intuitively reflected from the massive, large, and noisy data, and these data are more useful potential rules.

2. Research Methods

2.1. Concept of Data Mining Technology. Data mining technology refers to classifying and collecting the relevant data involved in a certain range and identifying and detecting the internal relationship and data law between the data. Data mining technology specifically includes three basic parts: data preparation, data law (Exploring the law of data), and data expression [8]. The data mining engine can be designed and classified according to the expected rules of the data set, so as to lay the foundation for the design of the data mining engine and the classification of the potential data set. In the era of big data, although data mining technology has certain advantages, the whole operation process is relatively complex and involves many steps, so it needs to be planned and prepared based on actual needs. Data mining technology focuses on data preprocessing. Therefore, the preprocessing stage is the basic stage of the application of the whole data mining technology, and its quality is also directly related to the final effect. The process structure of data mining technology (see Figure 2):

Through the analysis of the principles and characteristics of a variety of network security threats, combined with a variety of known data analysis methods and technologies, a number of new methods and new technologies of network security situation analysis based on data mining, such as event diffusion model, hotspot verification model, ternary model, and so on. These models can effectively analyze and process different data, including communication data known to determine network security threats, and metropolitan area network traffic communication data, such as the type of hot spot security events, and the development trend of network security events. The data source of the project comes from two parts: for the determined type of network security threat monitoring data, the text file generated by each system in advance; For man traffic data, the dynamic detection engine generates data, see Figure 3.

2.2. Relevant Key Technologies

2.2.1. Data Mining Technology. Among many key technologies, data mining technology is one of the most important technologies. Data mining technology is to extract data rules that are not easy to be intuitively reflected from massive large-scale noisy data. These data are more useful potential rules [9]. After data extraction, data preparation should be carried out. The data preparation process is cumbersome. This process is to explore and modify the data and provide a theoretical basis for the establishment of a data model after modification. After the completion of modeling, the model needs to be optimized, and the model should be continuously evaluated in the process of data analysis. After multiple rounds of optimization, the application strategy should be released, so as to complete all the work content of a data mining cycle. With the deepening of the user application, the strategy and model of data mining will be continuously optimized until the business rules are stable.

2.2.2. Security Settings Collection Technology. This technology belongs to data mining technology. This technology can set specific rules and frequent content columns in each process. Adopting this encryption technology can carry out an effective execution defense. During the exchange of an encryption algorithm, the encryption key can be any number between k1-kn, the last encrypted data M can be applied to all keys, each site will set a specific encryption column separately, and the last encryption strategy can be used by all sites so that the relevant columns of each site can be controlled effectively. Since the encryption technology is applied to the network site for exchange, the corresponding will encrypt the same column and comprehensively detect the global situation. Finally, the defense detection of each network site will make the content of each column encrypted.

2.3. Computer Network Security Maintenance System Based on Data Mining. The concept of this system was first put forward by Anderson in the 1980s. He believes that this technology is an upgrade of the computer review mechanism, and with the help of this technology, it can provide a secure defense mechanism for the inside of the computer. The main function of this system is to carry out real-time monitoring and control of computer virus intrusion, give early warning and deal with security related problems, and take relevant measures to reduce the risk coefficient. Its basic components are the data information acquisition module, analysis engine module, and response module. The main core business logic in the system is mainly realized based on decision number mining and association rule mining, as follows: this system has two attributes, one is relevance and the other is dissimilarity. In the system database, there are some attributes similar to the related function knowledge category. If the detected data is related to the original data, it indicates that there is a virus, which is the related attribute of this defense system [10]. After data collection, there will be obvious data with different attributes from other data in many data, which is called heterogeneous data or outliers. There are differences between heterogeneous data and normal data, but these data will not bring useless information to users. Some data may be garbage data, but some data may bring valuable content to users.

2.3.1. Decision Tree Mining. In essence, a decision tree is a tree structure. Its basic structure is similar to the table structure. Each node of the tree species represents the test of this nature. The branches between the nodes identify the

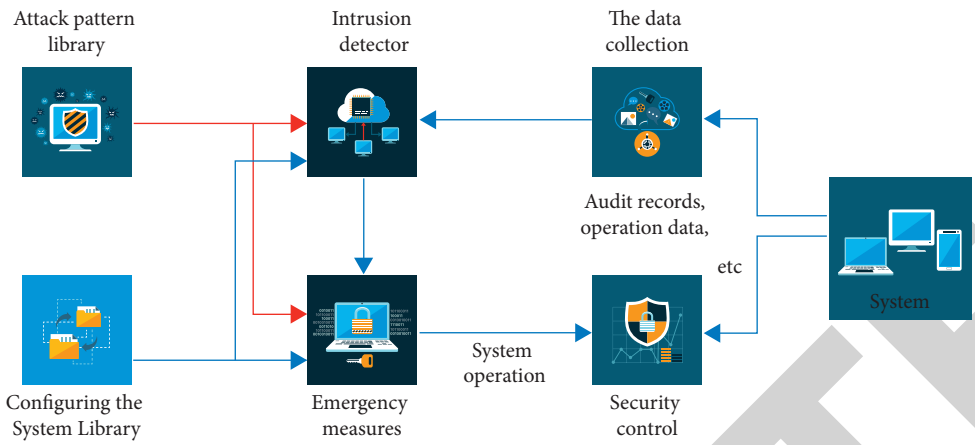

Figure 1: Data mining technology for network security.

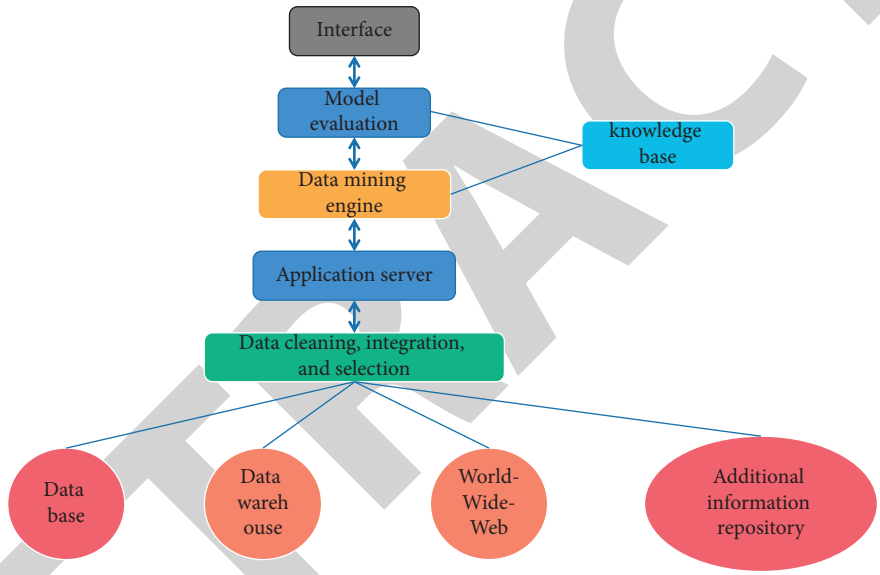

Figure 2: Data mining technology process structure.

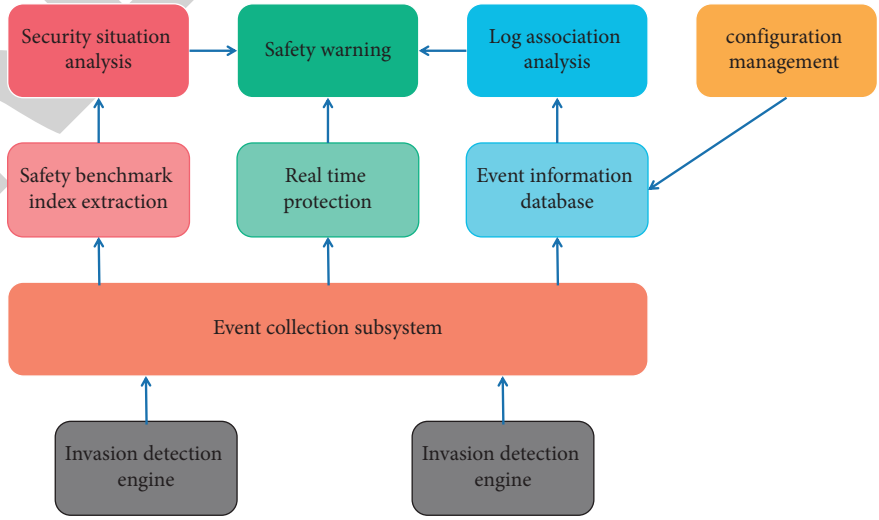

Figure 3: Function diagram of dynamic detection engine.

specific test results. Finally, different forms of state test results can be obtained on the final leaf node [11]. In the classification tree, the most basic and commonly used rules are ID3 and C45. The above two are carried out according to the bottom-up method, and the operation rule is $X1 + x2 = X$. The basic structure of the decision tree is shown in Figure 4.

2.3.2. Association Rule Mining. The main setting logic of association rules is that in many network site topologies, if the specific column is defined as $I = \{i1, i2, i3, \ldots, in\}$ and the processing value is set to $T = \{T1, T2 \ldots Tn\}$, then each Ti belongs to the column [12]. For any Ti, we can get that the X value belongs to the I set. The specific form of association rules is X- > Y ($X \cap Y = 0$) . Jiading's processing value C% in t is $X \cup$Y and C%, in which C% includes X and Y, the specific formula algorithm is as follows fd1:

$$\mathrm{SUP}(x) = \sum \mathrm{SUP}_1(X); \mathrm{CONF}(X \longrightarrow Y) = \frac{\mathrm{SUO}(X \cup Y)}{\mathrm{SUP}(X)}. \tag{1}$$

According to formula (1), it is the main method to carry out association rules for data mining.

2.3.3. Native Bayes Algorithm. Among the many algorithms of data mining, this algorithm is a more effective and feasible algorithm. At present, this algorithm has been applied to task division and area management, has been successfully applied in medicine and sales, and has successfully provided rich data mining and detection protection for all kinds of users [13]. This algorithm can be defined in this way. The attribute of specific event m is defined as A1 - am, and V is the specific attribute classification.

Any AI has its subset: $Ai = \{ai1, ai2 \ldots ain\}$. Each category V has its own domain $(v1, v2 \ldots vd)$. Classified data points tend to $(aj1, aj2 \ldots ajm, vj)$. Given a new example $(aj1, aj2 \ldots ajm)$, we can obtain the following equation fd2:

$$v = \mathrm{argmax} P\left(v^1\right) \prod_{i=1}^{m} P\left(a_i | v^i\right). \tag{2}$$

2.3.4. Model Establishment. With the continuous development of computer technology, Internet Finance, and e-commerce platforms have sprung up and are fully promoted and applied throughout the country. More and more platforms use data mining technology to carry out network detection and defense, so as to protect the core data assets of the protector from infringement. From 2013 to 2015, after the businesses of e-commerce Taobao and Jingdong Mall were absorbed, they began data detection and big data inspection and protection based on data mining, and carried out the application of specific algorithms. The establishment of the model is a specific solution for the prominent virus intrusion. If the relevant data from the website has the attribute v, it can be distinguished based on rules through classification and rule calculation. It can be seen that through the setting of the model, with the help of functions such as data classification and rule calculation, the prediction of viruses can be effectively prevented, and data can be collected as needed to carry out data defense work.

3. Result Analysis

As an important part of network technology, business recognition technology in a high-speed IP network has been valued by network management and users since the birth of the Internet. With the continuous emergence of P2P and various unknown services and encryption services, the traditional port number-based detection method has been unable to deal with the efficient and accurate identification of business flow, and DPI and DFI business flow identification technology has become a better way to solve this problem. According to the 41st China Internet Development Statistical Report released by the China Internet Information Center, by the end of 2021, the number of security vulnerabilities collected from the country's information security vulnerability sharing platform will reach 14,871, compared to 2020. Increased by 46.6%. There are 5,567 high-risk vulnerabilities, an increase of about 1,400 vulnerabilities compared to last year. Figure 5 shows the security vulnerabilities included in China's security vulnerability sharing platform in recent years. It can be seen that the number of vulnerabilities and high-risk vulnerabilities found every year are basically increasing year by year.

3.1. Application Process Analysis of Data Mining Technology in Network Security. There are many methods of data analysis. Traditional statistical methods such as classification and sum have provided important means for people's data analysis and still play an important fundamental role today. However, with the increasing complexity of data, these can no longer meet people's requirements to find more valuable information from massive data towels. With the continuous development of computer technology and the continuous integration with traditional statistical methods, the data mining technology produced by the combination of the two is gradually becoming a hot new means of data analysis today.

In essence, any network security problem actually has traces to follow, especially network viruses. Data mining technology mainly uses the corresponding means to reasonably classify, collect and evaluate the user's data, so as to dynamically scan the data of the whole system. It should be noted that the process of applying data extraction technology to protect against network security issues is relatively complex and often involves large amounts of data, so it is important to clearly understand the nature of the various links. Plan them into multiple modules to manage the modules. The process of applying data extraction technology to network security for in-depth analysis (see Figure 6).

3.2. Overview of Specific Modules Specific Modules Include

(1) The main function of this module is to intercept, resend, transfer, and edit the data packets transmitted and received by the network. After the data

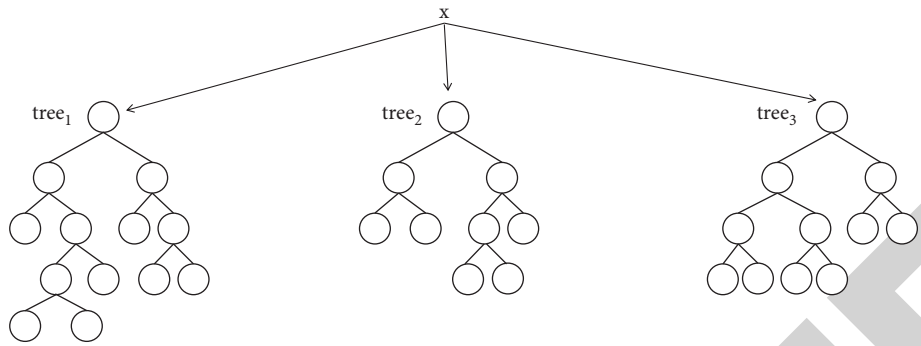

Figure 4: Basic structure of decision tree.

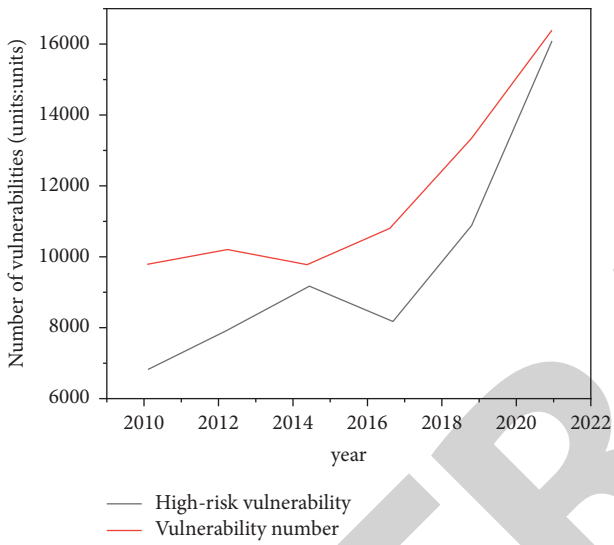

Figure 5: Number of security vulnerabilities and trend of high-risk vulnerabilities of national information security vulnerability sharing platform.

source module processes and transmits the original data packet, the data structure is sent to the preprocessing module and sent.

(2) Preprocessing module, which contains multiple data processing tools, can preprocess various types of data, so it is the key of data mining technology. Specifically, the preprocessing module includes feature standardization, minimum and maximum normalization of original data, normalization of change value mapping, and other steps, which can minimize the data mining time and reduce the mining cost [14].

(3) Data mining module, which processes and analyzes the information in the data warehouse with the help of information processing methods such as decision tree, genetic algorithm, fuzzy set, case-based reasoning, and statistical methods and then sends the information to the decision module.

(4) Rule base module, which can record the relevant characteristics of network security problems, such as network virus, malicious attack, abnormal intrusion, and other characteristics, summarize and classify them, and provide necessary theoretical support for network security defense.

(5) Decision module, the main function of this module is to match the data in the data mining module and the rule base module, that is to say, if the matching degree of some data in the two modules is relatively high, it means that there are hidden dangers of network security. For example, there may be network viruses in the data packets, so corresponding defense measures need to be taken.

3.3. Application Mechanism Analysis of Data Mining Technology in Network Security

3.3.1. About the Use of Data Collection. The use of data mining technology in network security is closely linked to computer technology, and data mining is based on computer technology. In the information age, data information is growing explosively, especially social communication will involve a lot of privacy. Therefore, it is very important to protect personal privacy in network security. Therefore, with the help of data mining technology, we can quickly find the hidden dangers of network security through data information. Taking the virus as an example, we can quickly find the program of virus code and clarify the unsafe information in the network virus in time, such as abnormal intrusion, malicious attack, and so on [15].

Network virus usually infiltrates the computer system in the form of code. In the process of destroying the system, the computer program has become the biggest support of network virus. Therefore, we should deeply analyze the code program through data mining technology, so as to clarify the problem and defend in time. Generally speaking, virus program code and computer software have certain commonalities and will invade into the system as users use the software. Data mining technology can collect, collect and classify network virus code programs by modules [16].

3.3.2. About the Use of Data Processing. In the process of network security defense, data mining technology can effectively mine and analyze data information and clarify the root cause of network security problems with the support of

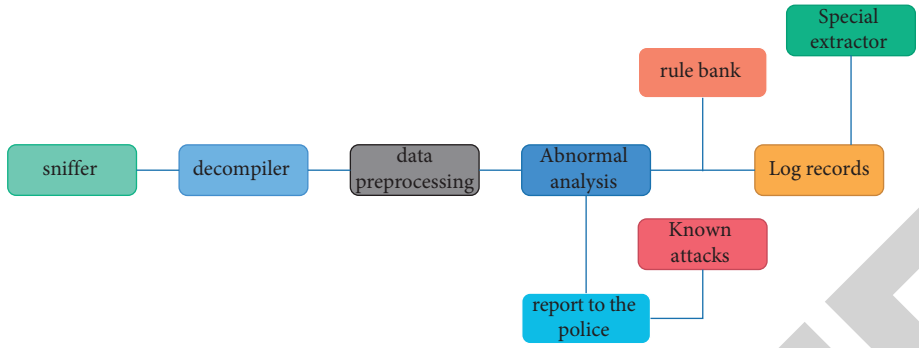

Figure 6: Application process of data mining technology in network security.

key information [17]. In terms of network security, it does not attack the computer system through text but mainly depends on the program code. Therefore, if we want to improve the defense of network security, we need to effectively convert and crack the network program code. In short, it is to enable it to convert to a recognizable mode, so that its program code can be cracked and defended in time [18]. The data processing module in data mining technology can identify and transform network security problems, including data source location and information, IP location and other data contents, and implement deep-seated mining, which can accurately locate the IP target, so as to find the root of network virus problems and then quickly block its transmission path, so as to avoid the continuous spread and spread of the virus. At the same time, data terminals are developed with the help of data mining technology, the purpose of which is to classify, analyze and organize information, which helps to analyze network security issues and reduce breakdown time, which is not only helpful for improvement. Ensure the efficiency of data mining technology, as well as information security during use [19].

3.3.3. About the Use of Database. The associated database can provide the function of cluster analysis for data mining technology and can be deeply identified according to the characteristics of network security problems. For example, when malicious behavior attacks the computer terminal system, the associated database can comprehensively record and summarize its running track, execution program, and basic characteristics [20–22]. In the whole process, the cluster analysis algorithm plays a very important role. It can make full use of attack rules to identify the characteristics of network viruses and strengthen the identification effect of the computer defense system.

3.3.4. On the Use of Decision-Making Mechanisms. Data mining technology plays a very important role in the application of network security. It will match the data in the data mining module and the rule base module. If the matching degree is relatively high, it means that there is a hidden danger of network security. At this stage, 360 firewall is generally installed in the process of computer use. Based on the function of 360 software, it can provide a great convenience for users. However, from the actual situation, the accuracy of the loudness of the 360 firewall is relatively low, which may lead to the wrong judgment of the attribute of the network virus. This is because the function of the decision module is not perfect enough so that the binding force of rule operation conditions is reduced. Taking the blackmail virus as an example, the encryption method library is implemented for the new blackmail virus, and the HTTP request of the script file can be realized. Reading according to the characteristics of the remote server file can effectively improve the efficiency of defending against network virus [23]. It should be noted here that although data mining technology can summarize virus characteristics in combination with data law characteristics, it must also have corresponding decision-making modules to solve network security problems. On the contrary, the system may misjudge, resulting in data type mismatch, leaving loopholes for the virus to invade the system and steal important information.

3.3.5. Scheme of Data Preprocessing. For the data preprocessing scheme, it is based on the decision-making conditions and virus characteristic information, so as to continuously improve the results and make them the final audit of analysis and classification, such as port information and induction of target IP address. In the process of network security defense, the relevant information of network security problems can be verified with the help of data preprocessing scheme, so as to provide valuable data parameters and verification indicators for the defense system [24–26]. Therefore, in the application process of data mining technology, through the judgment of the data preprocessing scheme, the original characteristics of network security problems can be accurately described, such as virus type, abnormal intrusion, system vulnerability, and malicious attack behavior, which can fully improve the defense ability of the system.

4. Conclusions and Outlook

To sum up, the network has been inseparable from people's life, work, entertainment, etc. Although the network has brought great convenience to people, it also brings certain

security issues. Personal privacy, corporate information, government agencies and units Important documents, etc., may be leaked, tampered with, or damaged due to network security issues. Therefore, it is necessary to strengthen the defense of network security. In the context of the era of big data, data mining technology has certain advantages. Using it in network security defense can fully improve the security level, especially in the defense of network viruses. Therefore, it is recommended to use data mining technology to strengthen promotion so that it can play a greater role. In the actual system platform construction, the model and algorithm application practice have a good verification effect and proved that it can use the computing advantages of the computer to help users obtain meaningful information from a large number of data. For example, the hot event discovery model found the absolute number of frequent network Trojan from the human network security event data. Of course, from a broader perspective, all the methods and means of research need further and more in-depth research and development.

From the perspective of the future development direction, the subsequent network security situation analysis method and technical research can be through several aspects to develop:

(1) New algorithms and technologies can be tried to gradually integrate data mining, such as association rules, time series technology, spatial topic algorithm, classification technology, outlier algorithm, and other. Some algorithms have good processing effects in the analysis of the human sequence.

(2) The characteristics of different network security monitoring data should be optimized, such as studying traffic monitoring and analysis based on address, protocol, routing, and monitoring, and early warning based on new network security threats, etc. For example, in the attack traffic analysis of MAN, the next step will be to further study the construction method and abnormal judgment method of the security benchmark index, and through a more comprehensive and more accurate benchmark index, it can better realize the situation assessment of the macro network security.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Farhadi, A. Esmaeily, and M. Najafzadeh, "Developing a decision tree based on data mining method for detecting the influential parameters on the power of flood destruction," *Amirkabir (Journal of Science and Technology)*, vol. 53, no. 5, p. 5, 2021.

[2] H. Asami, M. Golabi, and M. Albaji, "Simulation of the biochemical and chemical oxygen demand and total suspended solids in wastewater treatment plants: data-mining approach," *Journal of Cleaner Production*, vol. 296, no. 2-4, pp. 126533–126538, 2021.

[3] H. Moayedi, M. M. Abdullahi, H. Nguyen, and A. S. A. Rashid, "Comparison of dragonfly algorithm and Harris hawks optimization evolutionary data mining techniques for the assessment of bearing capacity of footings over two-layer foundation soils," *Engineering with Computers*, vol. 37, no. 1, pp. 437–447, 2021.

[4] T. Yang, L. Zhang, T. Kim, Y. Hong, D. Zhang, and Q. Peng, "A large-scale comparison of artificial intelligence and data mining (ai&dm) techniques in simulating reservoir releases over the upper Colorado region," *Journal of Hydrology*, vol. 602, no. 6, Article ID 126723, 2021.

[5] Y. Xiang and G. Yamamoto, "A data mining approach to investigate the carbon nanotubes mechanical properties via high-throughput molecular simulation," *Materials Science Forum*, vol. 1023, pp. 29–36, 2021.

[6] E. P. Booker and G. E. Jabbour, "Antiviral nanoparticle ligands identified with datamining and high-throughput virtual screening," *RSC Advances*, vol. 11, no. 37, pp. 23136–23143, 2021.

[7] Y. Li, R. K. Shyamasundar, and X. Wang, "Special issue on computational intelligence for social media data mining and knowledge discovery," *Computational Intelligence*, vol. 37, no. 2, pp. 658-659, 2021.

[8] Y. Liu, Z. Yu, and Y. Yang, "Diabetes risk data mining method based on electronic medical record analysis," *Journal of Healthcare Engineering*, vol. 2021, no. 6, pp. 1–11, 2021.

[9] K. Yu, W. Shi, and N. Santoro, "Designing a streaming algorithm for outlier detection in data mining—an incrementa approach," *Sensors*, vol. 20, no. 5, p. 1261, 2020.

[10] N. Bellin, E. Racchetti, C. Maurone, M. Bartoli, and V. Rossi, "Unsupervised machine learning and data mining procedures reveal short term, climate driven patterns linking physico-chemical features and zooplankton diversity in small ponds," *Water*, vol. 13, no. 9, p. 1217, 2021.

[11] B. Wu, D. Qin, J. Hu, and Y. Liu, "Experimental data mining research on factors influencing friction coefficient of wet clutch," *Journal of Tribology*, vol. 143, no. 12, pp. 1–14, 2021.

[12] S. Bardak, T. Bardak, H. Peker, E. Sözen, and Y. Çabuk, "Predicting effects of selected impregnation processes on the observed bending strength of wood, with use of data mining models," *Bioresources*, vol. 16, no. 3, pp. 4891–4904, 2021.

[13] R. Wang, "Exploration of data mining algorithms of an online learning behaviour log based on cloud computing," *International Journal of Continuing Engineering Education and Life Long Learning*, vol. 31, no. 3, p. 371, 2021.

[14] J. Gao, X. G. Yue, L. Hao, M. J. C. Crabbe, O. Manta, and N. Duarte, "Optimization analysis and implementation of online wisdom teaching mode in cloud classroom based on data mining and processing," *International Journal of Emerging Technologies in Learning (IJET)*, vol. 16, no. 01, p. 205, 2021.

[15] I. Parvez, J. Shen, I. Hassan, and N. Zhang, "Generation of hydro energy by using data mining algorithm for cascaded hydropower plant," *Energies*, vol. 14, no. 2, p. 298, 2021.

[16] J. Li, "Analysis of the mental health of urban migrant children based on cloud computing and data mining algorithm models," *Scientific Programming*, vol. 2021, no. 5, pp. 1–7, 2021.

[17] N. Suo and Z. Zhou, "Computer assistance analysis of power grid relay protection based on data mining," *Computer-Aided Design and Applications*, vol. 18, no. S4, pp. 61–71, 2021.
[18] P. Chen and L. Yu, "Use of data mining technologies in an English online test results management system," *International Journal of Emerging Technologies in Learning (IJET)*, vol. 16, no. 09, p. 166, 2021.
[19] B. Wang, "Multimedia filtering analysis of massive information combined with data mining algorithms," *Advances in Multimedia*, vol. 2021, no. 3, 7 pages, Article ID 7461874, 2021.
[20] H. Vajjha and P. Sushma, "Techniques and limitations in securing the log files to enhance network security and monitoring," *Solid State Technology*, vol. 64, no. 2, pp. 1–8, 2021.
[21] S. Einy, C. Oz, and Y. D. Navaei, "The anomaly- and signature-based ids for network security using hybrid inference systems," *Mathematical Problems in Engineering*, vol. 2021, no. 9, 10 pages, Article ID 6639714, 2021.
[22] H. Zhang, X. Meng, X. Zhang, and Z. Liu, "Cansec: a practical in-vehicle controller area network security evaluation tool," *Sensors*, vol. 20, no. 17, p. 4900, 2020.
[23] Q. Liu and M. Zeng, "Network security situation detection of internet of things for smart city based on fuzzy neural network," *International Journal of Reasoning-Based Intelligent Systems*, vol. 12, no. 3, p. 222, 2020.
[24] J. Huang, W. Huang, Z. Meng, F. Miao, and Y. Xiong, "Static analysis of superfluous network transmissions in android applications," *International Journal on Network Security*, vol. 22, no. 3, pp. 411–420, 2020.
[25] Y. Wang, J. Ma, A. Sharma et al., "An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks," *Journal of Sensors*, vol. 2021, no. 3, 11 pages, Article ID 5558860, 2021.
[26] N. Sun, T. Li, G. Song, and H. Xia, "Network security technology of intelligent information terminal based on mobile internet of things," *Mobile Information Systems*, vol. 2021, no. 8, 9 pages, Article ID 6676946, 2021.