Research Article

Prediction of Computer Network Security Situation Based on Association Rules Mining

Rixin Xue ¹, Peng Tang,¹ and Shudong Fang²

¹College of Big Data and Artificial Intelligence, Chizhou University, Chizhou 247000, Anhui, China

²College of Mechanical and Electrical Engineering, Chizhou University, Chizhou 247000, Anhui, China

Correspondence should be addressed to Rixin Xue; xrxscp@czu.edu.cn

Received 30 December 2021; Revised 18 January 2022; Accepted 19 January 2022; Published 9 February 2022

Academic Editor: Xin Ning

Copyright © 2022 Rixin Xue et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Traditional NSSA (network security situational awareness) systems have significant equipment limitations, poor data fusion capabilities, and a low level of analysis and evaluation, making them difficult to adapt to large-scale and complex network environments. This paper proposes the study of computer NSS (network security situation) prediction technology based on AR (association rules) mining to solve this problem. The support-confidence framework is improved by introducing an interest evaluation standard, and the value of AR is re-evaluated, based on a discussion of traditional concepts and algorithms related to AR mining. The MFP-interest algorithm proposed in this paper is a combination of alarm AR template and interest degree. The MFP-interest algorithm was put to the test. We discovered that the MFP-interest algorithm can effectively predict NSS and indicate its development trend when run in a real-world network environment. Most time points have a relative error range of less than 0.035.

1. Introduction

With the increasing popularity of all kinds of information networks, network risks are increasing, network viruses are frequently attacked, network intrusion is inevitable, and network security problems are becoming increasingly serious. Including hacker attacks, the vulnerability of network security is gradually exposed [1]. Using traditional methods alone may be inadequate, which not only harms the interests of individuals and enterprises and causes the loss of people's property but also reduces people's trust in the network [2, 3]. In view of the fact that the network security situation has become a key issue in the field of network security, knowing the network security situation has become an important means to ensure the network environment security and suppress the hidden network security threats in communication.

People have implemented network security protection measures, such as firewall technology, intrusion detection technology, VPN technology, and so on, in response to such frequent network mishaps [4–6]. Although each

technology has played a role in network security, it has flaws and can no longer meet people's current needs. Real-time network security situation assessment, prediction of NSS (network security situation), and its trend, in order to actively control the network before security incidents occur, avoiding damage and ensuring the integrity and security of network resources [7]. Because of China's rapid development of Internet-related industries, relevant security mechanisms have not been implemented in a timely manner. Although the Internet makes information transmission, storage, and retrieval easier, the security of the interconnection and sharing process has not been adequately guaranteed. Because there is a significant gap between existing network security protection measures and current needs, it is critical to develop a new security protection measure, and NSSA (Network Security Situational Awareness) technology was born out of this need. It is determined whether it belongs to network potentially dangerous data through network data preparation, network abnormal data searching, and summarizing the law of network abnormal data.

Although many experts in our country have put forward the network security risk detection model based on artificial intelligence technology [8, 9], the number of NSS values that can be given by this kind of model is still too small, and there are quite some problems in its design and management, which can only detect certain network vulnerabilities with great limitations and cannot detect the whole network, so this algorithm plays a very limited role in improving network security. In this paper, a new NSSA system is designed and implemented by deeply studying the key technology of computer NSS prediction based on AR (association rules) mining. Research on computer NSS prediction technology based on AR mining is committed to ensure the landing of NSSA security capability through decision-making and action.

2. Related Work

Many scholars and experts in the United States and abroad have conducted extensive research on network security, which can be divided into misuse detection and anomaly detection based on various detection methods [10, 11]. Many scholars have devoted themselves to research in this field, primarily in two aspects: NSS evaluation and NSS prediction, as evidenced by literature [11]. The process of network service anomaly detection was transformed into a hidden Markov model in literature [12], and the data test revealed that the model had a good recognition rate for network service anomaly. Literature [13] proposed a Bayesian network-based situation assessment model for multivariate data fusion. A threat prediction and situation awareness model based on game theory is proposed in the literature [14]. First, threats are detected by software, followed by information fusion, and finally, the attack intention is predicted using a discrete hidden Markov game model. Literature [15, 16] examines the performance indexes of various kernel functions and use them to predict SVM (support vector machine). A hidden Markov game model is established based on the analysis of threats, administrators, and users' behaviors. Experiments show that this model can dynamically reflect network security conditions and provide administrators with a decision-making basis. According to the potential relationship between situation and security incidents, literature [17] establishes a Bayesian network evaluation model and expounds the corresponding information dissemination algorithm. Finally, an example is given to demonstrate the Bayesian network calculation process.

Compared with the traditional methods such as viruses and phishing websites in the past, the threats of the network are not limited to these less harmful means, and the attackers' use of weak links in the network tends to be more complicated and hidden. This makes the network defense more difficult. Literature [18] describes and studies the new algorithms and technologies of large-scale complex network behavior visualization, focusing on the dynamics of network and the uncertainty of network data. Literature [19] points out two key technologies-multisensor data fusion and data mining. Literature [20] puts forward a hierarchical quantitative evaluation model of security situation based on

statistical analysis, which is divided into four levels from top to bottom: system, host, service, and attack/vulnerability and adopts the evaluation strategy and corresponding calculation method from bottom to top, first local and then overall. Literature [21] developed a set of NSS evaluation system based on LAN, which consists of two parts: network security risk status evaluation and network threat development trend prediction, and is used to evaluate the vulnerability and security threat level of network equipment and structures.

Based on the current state of domestic research, it can be seen that domestic research primarily focuses on situation assessment, with less research on situation prediction. Different evaluation methods are used by different researchers. It is difficult to judge the quality of a particular situation evaluation method due to the strong subjectivity of situation evaluation methods and the lack of uniform evaluation standards.

3. Research Method

3.1. Establishment of NSSA System. NSSA is the ability to comprehensively analyze the external environment dynamics, so as to perceive the existence of security risks [22]. NSSA takes big data as its core technology and is an effective way to identify, analyze, and deal with potential threats to network security from the overall perspective. Data mining refers to the process of automatically mining out potentially dangerous network data hidden in a large number of network data. By preparing network data, searching for abnormal network data and summarizing the law of abnormal network data, it can be judged whether it belongs to potentially dangerous network data.

The network security situation can no longer be reduced to a qualitative assessment. It requires a reasonable, effective, and accurate quantitative assessment of the current network security situation in real time in order to detect hidden network dangers quickly, provide a solid foundation for forecasting network security trends, and reduce network security threats. Establish a problem-solving system that is relevant to achieving a quantitative assessment of the security situation. To ensure high adaptability, the evaluation model must be able to assess both individual and group attack forms in the network, as well as express the security situation intuitively in digital form. The ultimate goal of system research and development is to create an integrated NSSA and trend analysis system to protect network information security, as well as a foundation for network supervisors to understand network status in real time and formulate network security policies. The NSSA system creates the NSSA model, which classifies, describes, calculates, and analyzes the safety indicators. Not only can the security situational awareness model reflect the current state of network security, but it can also self-learn. It can deduce changing rules from changes in network security indicators and forecast the NSS's changing trend.

This system is mainly used for the situation awareness and prediction of macro network. In the large-scale network environment, how to fully acquire the basic elements of the network and make comprehensive analysis is the main

problem to be solved in the system design. In view of the characteristics of large scale and large amount of data in macro network, build a distributed multilayer system structure, which mainly includes two parts: information collection terminal and analysis center. The hierarchical diagram of the whole system is shown in Figure 1.

Each information collection terminal in the system is distributed among the large-scale network's key nodes and is in charge of collecting and sorting the network's basic data, extracting the features that can represent the network state from it, and counting these features according to the index format. The situation awareness center is in charge of receiving network indicator data from each terminal, analyzing the data comprehensively using a situation assessment algorithm, and determining network state changes. Simultaneously, the situation prediction algorithm is used to forecast the network situation's changing trend.

Includes the data body to be transmitted by the interface, protocol identification, source address, destination address, source port identification, and destination port identification. The structure is shown in Figure 2.

Situation assessment is a qualitative and quantitative description of network security that is at the heart of situation awareness and auxiliary analysis. To obtain the relevant information for evaluating individual assets, threats, vulnerabilities, and security events in the network, statistical analysis is performed on the asset data set, threat data set, and security event data set obtained from situation understanding. The system's situation assessment module uses hierarchical and multidimensional security situation assessment technology to divide the security situation assessment process of the entire network management domain into asset assessment, vulnerability assessment, security incident assessment, threat assessment, and security situation assessment, resulting in the overall state and situation of the network management domain.

After the prediction model is generated, the system will automatically call the corresponding data for prediction according to the needs of the model. Because the model contains a variety of prediction algorithms, many prediction data will be generated. In order to get the best prediction effect, the system will calculate the weighted average of this group of data according to the historical accuracy of the results produced by each algorithm and comprehensively get the most ideal result, which will be output as the final prediction data.

3.2. Computer NSS Prediction. AR mining is to dig out valuable knowledge describing the relationship between data items from a large amount of data. With the increasing scale of data collected and stored in the database, people are more and more interested in mining relevant knowledge from these data. There are two main steps in mining AR:

- (1) Frequent item sets found. Find all frequent item sets through the minimum support $\min_supp$ given by the user.

FIGURE 1: System structure hierarchy diagram.

FIGURE 2: Structure diagram of multiprotocol data communication framework.

- (2) Generate AR. According to the minimum confidence $\min_conf$ given by the user, AR $\min_conf$ with confidence not less than is found in each maximum frequent item set.

The specific description is

$$\begin{aligned} \text{support}(A \Rightarrow B) &= P(A \cup B), \\ \text{confidence}(A \Rightarrow B) &= P(B \cup A). \end{aligned} \quad (1)$$

In these two steps, the first step is to quickly and efficiently find out all frequent item sets, which is the central problem of AR mining and the standard to measure the performance of AR mining algorithm. The solution of the second step is relatively easy and direct. At present, most AR mining algorithms are proposed for the subproblem of the first step.

Obtaining information about the situation in the field of network security refers to the process of extracting valuable and important information about the state of network security from large-scale data sources, which serves as the foundation for quantitative perception and prediction of the situation [23]. The form and accuracy of quantitative perception are directly affected by the obtained objects and results. The research in this field of technology is still in its early stages, and there is a paucity of relevant research literature. However, early work on feature recognition, classification analysis, and clustering laid the groundwork for future research in this field.

The specific flow of computer NSS prediction technology based on AR mining designed in this paper is divided into three steps, as shown in Figure 3.

The feature extraction method of fractional interval spectrum is used to extract the features of NSS, and the virus information of end users is extracted. For a given single-component NSS time sampling sequence x_i , the cluster $d_{ij} \leq \varepsilon$ between its feature points is calculated to be $N(i)$, and the quantitative recursive entropy ratio $R_m(r, i)$ of the original NSS is obtained by quantitative recursive analysis.

$$R_m(r, i) = \frac{N(i)}{N - (m - 1)\tau}. \quad (2)$$

The vector space embedding dimension of NSS sequence is obtained. Under the condition of characteristic disturbance, the channel equalization model of NSS is as follows:

$$\text{ApEn} = \lim_{N \rightarrow \infty} [\text{AV}_m(r) - \text{AV}_{m+1}(r)]. \quad (3)$$

Alarm events come from alarm records of several security components in the network environment with different formats. Obviously, the alarm log is a multidimensional record, and mining AR of the alarm log should be attributed to mining multidimensional AR in the alarm log database.

In this chapter, FP-growth algorithm is evolved into MFP-growth (multidimensional FP-growth) algorithm for mining multidimensional AR [24], and then AR template and interest degree are further developed to constrain multidimensional AR mining, which is called MFP-interest method.

For AR $X \Rightarrow Y$, support is defined as

$$\text{support}(X \Rightarrow Y) = P(X \cup Y). \quad (4)$$

Confidence is defined as

$$\text{confidence}(X \Rightarrow Y) = \frac{P(X \cup Y)}{P(X)}. \quad (5)$$

The AR that meets the minimum support and confidence becomes a strong AR, although using the minimum support threshold and the minimum trust threshold can help eliminate or reduce mining meaningless rules.

Interest is defined as

$$\text{interest}(X \Rightarrow Y) = \frac{P(X \cup Y)}{P(X) \cdot P(Y)}. \quad (6)$$

AR degree of interest is a measure of conciseness, certainty, practicality, and novelty of rules.

Therefore, in the process of AR mining, the minimum support setting is required to be as low as possible, which puts forward higher requirements for the performance of mining algorithms, and when the minimum support setting is low, the proliferation of a large number of useless rules seriously affects the usability of AR mining; AR template can limit the generation types of AR, only generate rules that users are interested in, and greatly reduce the generation of useless rules. The MFP-interest algorithm in this paper is put forward under the above circumstances.

The MFP-interest algorithm uses FP tree, a compressed data storage structure in the MFP-growth algorithm, and adopts the following divide-and-conquer strategy:

Compress the alarm log library providing frequent item sets into a frequent pattern tree FP-tree and keep the frequency count and dimension attributes of item sets.

The compressed database is then split into a set of conditional databases, the original large database is divided into several data subsets based on the frequent patterns discovered, and longer frequent patterns are created by combining local frequent patterns. In the process of frequent pattern growth, an AR template is used to constrain pattern growth; only the patterns required by the template are generated, and the template's support is calculated, which not only eliminates a large number of unnecessary frequent item sets but also greatly accelerates the algorithm's convergence speed and improves performance.

To summarize, the AR mining-based computer NSS prediction process can be thought of as a method of determining the law among potentially dangerous data in the network security operation dimension situation matrix. The NSSA threshold is set by data mining, and only data with NSS commonality are selected for mining [9]. To the greatest extent possible, distinguish the similarities and differences between potentially dangerous data in the network and avoid the false perception caused by similarity. The computer NSS prediction technology based on AR mining has been completed up to this point.

4. Results Analysis and Discussion

It is an open and shared operating platform of the Internet. Data and information can be transmitted and shared in the network state, which meets people's demand for information resources and reduces the acquisition cost of information resources. While the computer network brings convenience to people's work and life, it also provides opportunities for criminals. No matter what kind of malicious attack, the computer network will be threatened by security. For this reason, hackers have become the primary influencing factor of computer network security in the era of big data.

To avoid economic losses caused by malicious information theft in the age of big data, computer users should improve their network security awareness. To avoid the leakage of personal information caused by criminals using virus programs to collect information, users should regulate

FIGURE 3: Flow chart of computer NSS prediction technology based on AR mining.

their computer network use behavior, do not click on unsafe web links at will, and cannot upload personal information without first confirming its safety. Furthermore, to prevent criminals from maliciously invading users' computers, computer users should set access rights to the home network. Users should immediately seek the assistance of professional network maintenance personnel to repair the computer system if they discover password leakage or abnormal computer system operation.

In this experiment, the MApriori algorithm, MFP-growth algorithm, and MFP-interest algorithm are used to mine frequent item sets for alarm log databases of different sizes, and their running time is compared. Figure 4 shows the performance comparison of small-scale alarm log mining algorithms.

It can be clearly seen in Figure 4 that the performance of MFP-growth algorithm and MFP-interest algorithm is far better than that of MApriori algorithm. Therefore, MApriori algorithm is not suitable for mining massive alarm logs.

The network equipment information is entered into the asset database by manual registration and merged with the data collected by the data collector. The network vulnerability information, vulnerability information, and other data are simply processed by the data collector and entered into the network security basic database. The network security event database is formed by correlation analysis. The analysis results form a basic fuzzy matrix. The NSS is evaluated by the method of combining the analytic hierarchy process with the fuzzy matrix. After the evaluation, the basic information details and evaluation results are displayed.

The original data are processed and stored in the database through data collection by various data collectors, and the security events are associated and analyzed to form the security event data stored in the database during the NSS evaluation process. The comprehensive evaluation of the entire NSS is obtained by analyzing the original data, and security events are responded to. Simultaneously, click a node to see the network security situation and calculate the current regional network's rating.

In practice, the scale of alarm logs is often very large, and massive alarm logs put forward higher performance requirements for mining algorithms. Because of the large-scale alarm log, when the minimum support threshold setting is low, MApriori algorithm cannot complete the mining task in a limited time. Figure 5 is a comparison of the running time

FIGURE 4: Performance comparison of small-scale alarm log mining algorithms.

FIGURE 5: Comparison of mining time of massive alarm logs.

of MFP-growth algorithm and MFP-interest algorithm in mining frequent item sets.

It is easy to see in Figure 5 that when the alarm log scale increases gradually, the running time of the algorithm increases gradually, but the MFP-growth algorithm takes more time than the MFP-interest algorithm with associated template constraints.

Various types of network security devices, such as intrusion detection systems, firewalls, and so on, generate a large amount of data information when the network is running, resulting in a large amount of log data. These disparate data must be preprocessed in real time to create a unified data format that can be stored and analyzed later. Different protocols supported by different network devices may differ, so different data collectors must be designed for data collection and must follow different protocols. Most network security device data can be gathered using the Syslog data collection protocol.

In Figure 6, with the increasing of alarm log scale, the memory consumption of algorithm running also gradually increases, and the MFP-interest algorithm with associated template constraint consumes less memory than MFP-growth algorithm.

The acquisition of network structure information consists primarily of network topology data as well as the association and improvement of equipment data on topology nodes. The index system configuration module is primarily responsible for configuring NSS's first- and second-level indicators, as well as dynamically configuring network security indicators and entering the NSS evaluation dictionary. Simultaneously, the extension function is provided, which provides an interface for future index system extension. The indicator system primarily depicts the hierarchical relationship between indicators and their corresponding data sources, as well as obtaining indicator data via the interface.

Figure 7. With the increasing scale of alarm logs, the number of frequent item sets in mining results is also increasing. The number of frequent item sets generated by MFP-growth algorithm without association template constraints far exceeds that generated by MFP-interest algorithm.

A large amount of alarm information collected by data collectors is stored in the basic database after being processed. It is necessary to analyze the security event information in it and remove redundant alarm information. The information contained in the alarm is closely related to the attack threats in the network. The task of network management analysis is to analyze the network security alarm, and analyze, denoise, and classify the alarm data. In association analysis, it is necessary to make association analysis of network security alarm information, call similarity function, form processed security event data, store it in security database, and form statistical analysis results.

Compared with other two prediction models (ref. [17] and ref. [19]), this method can improve the prediction accuracy. The specific data are shown in Figure 8.

Figure 8 shows that the method proposed in this paper provides the most accurate prediction, while other prediction methods have flaws. The data collected in the NSS

FIGURE 6: Comparison of peak memory usage in massive alarm log mining.

FIGURE 7: Comparison of mining frequent item sets.

evaluation module's main data collection process are statistically analyzed using the statistical analysis database and the key analysis security event database created by statistical analysis, and the calculation module is used to perform NSS evaluation. When a security threat is detected in the system, a specific response strategy is implemented. The system adopts internal response measures based on the NSS evaluation results, and then sends system threat information to the network security administrator. The linkage response must be called by plug-in by analyzing and comparing response times, taking appropriate measures, and sending e-mail.

Figure 9 is a comparison of the relative errors of different prediction methods at each time node. It can be seen that the prediction method in this paper is relatively stable in relative

FIGURE 8: Comparison of NSS values of different forecasting methods.

FIGURE 9: Comparison of relative errors of different prediction methods at different time nodes.

errors, and the relative error range of most time points is controlled within 0.035.

It can be seen from Figure 9 that the algorithm proposed in this paper has maintained a relatively high level under three error indicators, which reflects the accuracy of prediction.

The system data preprocessing module needs to standardize similar events from different event sources, merge redundant data from massive data, extract key information, form network alarm events, and provide data for correlation analysis of system security events. Through correlation analysis, the event analysis module can find the correlation between alarm events, merge security events in different

FIGURE 10: Prediction comparison of different improved SVM algorithms.

attack stages and multiple redundant alarm events, reduce the redundancy of events, and present complete security events and attack scenes of events to security administrators.

The above is a comparison with other prediction models, and then it will be compared with other SVM optimization algorithms, namely DE(Differential Evolution), ACO(Ant Colony Optimization) and PSO(Particle Swarm Optimization). Figure 10 is a comparison of prediction of different improved SVM algorithms.

From Figure 10, it can be seen that the prediction accuracy of different SVM optimization algorithms at each time point has a good performance. Although the above methods have some effect on SVM optimization, the global search ability is unstable due to the problems of algorithm mechanism or strategy. This algorithm meets the requirements of individual population at different stages, avoids falling into local optimum, and accelerates the convergence speed of the algorithm.

The prediction model will be generated automatically based on the user's requirements. The system will automatically determine the type of input indicators, the number of historical data calls, and the size of the predicted time range after the user inputs the prediction object, prediction intensity, and prediction accuracy. If the user's demand shifts, the model configuration parameters can be tweaked to create a new prediction model with the best prediction effect. How much historical data are called is determined by the number of samples. The module provides users with a configuration interface. According to their own needs, users can select appropriate parameters to meet the corresponding prediction requirements. The system default configuration will be used if users do not configure. It creates a new time series with the historical situation value after predicting the network situation value in the future period. Users can more intuitively understand the trend of network development and prepare for possible network security incidents by

analyzing and calculating various statistical characteristics of the sequence, such as trend characteristics and periodic characteristics.

5. Conclusion

To summarize, as the era of big data officially begins, people are paying increasing attention to computer network security. Users will suffer irreparable losses if a large amount of important information is lost or stolen from the computer network. In this paper, it is demonstrated that the NSSA precision of design technology is much higher than that of traditional technology, and that the designed perception technology can realize accurate perception of NSS, which can become the platform support for NSS information fusion and intelligent evaluation, and provide real-time and reliable management decision basis for network security managers, through research of computer NSS prediction technology based on AR mining. MFP-growth algorithm has higher nonlinear operation and mapping ability than traditional prediction methods, can approximate functional relationships with arbitrary accuracy, has strong adaptability, and has higher NSS prediction accuracy.

The outcome of the situation assessment affects NSS predictions. The results of the situation assessment will have a significant impact on the NSS prediction results if there is a significant deviation in the results. The index data can be predicted first, and the predicted index data can then be used to evaluate the predicted situation value.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

All the authors do not have any possible conflicts of interest.

Acknowledgments

This study was supported by Anhui University Provincial Natural Science Research Project (no. KJ2018A0582).

References

- [1] H. Zhang, C. Kang, and Y. Xiao, "Research on network security situation awareness based on the LSTM-DT model," *Sensors*, vol. 21, no. 14, p. 4788, 2021.
- [2] P. Yue and L. Zhao, "Research on the design of network security situation sensor based on network traffic," *Boletin Tecnico/Technical Bulletin*, vol. 55, no. 7, pp. 554–561, 2017.
- [3] C. Huang and C. Wang, "Network security situation awareness based on the optimized dynamic wavelet neural network," *International Journal on Network Security*, vol. 20, no. 3, pp. 593–600, 2018.
- [4] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2018.
- [5] B. Zhu, Y. Chen, and Y. Cai, "Three kinds of network security situation awareness model based on big data," *International Journal on Network Security*, vol. 21, no. 1, pp. 115–121, 2019.
- [6] P. Lu, S. Guo, H. Zhang et al., "Research on improved depth belief network-based prediction of cardiovascular diseases," *Journal of Healthcare Engineering*, vol. 2018, Article ID 8954878, 9 pages, 2018.
- [7] X. Meng, L. Nie, and J. Song, "IoT individual privacy features analysis based on convolutional neural network," *Cognitive Systems Research*, vol. 57, no. OCT, pp. 126–130, 2019.
- [8] J. Kong, C. Yang, J. Wang et al., "Deep-stacking network approach by multisource data mining for hazardous risk identification in IoT-based intelligent food management systems," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 1194565, 16 pages, 2021.
- [9] X.-B. Jin, W.-Z. Zheng, J.-L. Kong et al., "Deep-learning temporal predictor via bidirectional self-attentive encoder-decoder framework for IOT-based environmental sensing in intelligent greenhouse," *Agriculture*, vol. 11, no. 8, p. 802, 2021.
- [10] W. Zheng, "Research on situation awareness of network security assessment based on dempster-shafer," *MATEC Web of Conferences*, vol. 309, no. 10, Article ID 02004, 2020.
- [11] Z. Ran, L. Min, Y. Yifeng, Z. Qikun, and C. Zengyu, "Prediction algorithm for network security situation based on BP neural network optimized by SA-SOA," *International Journal of Performability Engineering*, vol. 16, no. 8, p. 1171, 2020.
- [12] 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.
- [13] P. Lin and Y. Chen, "Network security situation assessment based on text SimHash in big data environment," *International Journal on Network Security*, vol. 21, no. 4, pp. 699–708, 2019.
- [14] Y. Zhu and Z. Du, "Research on the key technologies of network security-oriented situation prediction," *Scientific Programming*, vol. 2021, Article ID 5527746, 10 pages, 2021.
- [15] M. Peng, S. Li, X. Liu, and W. Qu, "Research on prediction of development of computer network technology industry based on support vector machines," *Revista de la Facultad de Ingenieria*, vol. 32, no. 9, pp. 1–7, 2017.
- [16] N. Ta, H. Li, S. Liu, and Y. Zuo, "Mining key regulators of cell reprogramming and prediction research based on deep learning neural networks," *IEEE Access*, vol. 8, 2020.
- [17] X. Qiao, "Study on the computer network security evaluation based on GABP algorithm," *Boletin Tecnico/Technical Bulletin*, vol. 55, no. 18, pp. 497–504, 2017.
- [18] F. Catal, N. Tcholtchev, E. Höfig, and A. Hoffmann, "Visualization of traffic flows in a simulated network environment to investigate abnormal network behavior in complex network infrastructures," *Procedia Computer Science*, vol. 151, pp. 279–286, 2019.
- [19] C. Yang, A. Mohammadi, and Q.-W. Chen, "Multi-sensor fusion with interaction multiple model and chi-square test tolerant filter," *Sensors*, vol. 16, no. 11, p. 1835, 2016.
- [20] J. Liu and W. Fan, "Research on security situation assessment algorithm under virtual technology of cloud platform," *MATEC Web of Conferences*, vol. 336, no. 1, Article ID 08004, 2021.
- [21] R. Hou, G. Ren, C. Zhou, H. Yue, H. Liu, and J. Liu, "Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things," *Computer Communications*, vol. 158, pp. 64–72, 2020.

- [22] S. Yang, D. Yin, X. Song et al., "Security situation assessment for massive MIMO systems for 5G communications," *Future Generation Computer Systems*, vol. 98, pp. 25–34, 2019.
- [23] L. Wen, "Security evaluation of computer network based on hierarchy," *International Journal on Network Security*, vol. 21, no. 5, pp. 735–740, 2019.
- [24] P. Wei and Z. Zhou, "Research on security of information sharing in Internet of Things based on key algorithm," *Future Generation Computer Systems*, vol. 88, no. NOV, pp. 599–605, 2018.