Research Article

Ying Zhou, Guodong Zhao, Roobaea Alroobaea, Abdullah M. Baqasah, and Rajan Miglani*

Research on data mining method of network security situation awareness based on cloud computing

https://doi.org/10.1515/jisys-2022-0037
received December 04, 2021; accepted February 26, 2022

Abstract: Due to the complexity and versatility of network security alarm data, a cloud-based network security data extraction method is proposed to address the inability to effectively understand the network security situation. The information properties of the situation are generated by creating a set of spatial characteristics classification of network security knowledge, which is then used to analyze and optimize the processing of hybrid network security situation information using cloud computing technology and co-filtering technology. Knowledge and information about the security situation of a hybrid network has been analyzed using cloud computing strategy. The simulation results show that a cyber security crash occurs in window 20, after which the protection index drops to window 500. The increase in the security index of 500 windows is consistent with the effectiveness of the concept of this document method, indicating that this document method can sense changes in the network security situation. Starting from the first attacked window, the defense index began to decrease. In order to simulate the added network defense, the network security events in the 295th time window were reduced in the original data, and the defense index increased significantly in the corresponding time period, which is consistent with the method perception results, which further verifies the effectiveness and reliability of this method on the network security event perception. This method provides high-precision knowledge of network security situations and improves the security and stability of cloud-based networks.

Keywords: cloud computing technology, network, security situation, perception, data mining technology

1 Introduction

With the development of information technology, network technology has been closely related to people's lives and social development. Currently, network development is facing many critical problems; among them, network security issues are the most distressing [1]. Various cyber threats and attacks continue to be

* **Corresponding author: Rajan Miglani,** School of Electronics and Electrical Engineering, Lovely Professional University, Punjab, India, e-mail: rajanmiglani1028@gmail.com
Ying Zhou: Department of Science and Technology, Tianjin Open University, Tianjin, 300191, China, e-mail: zhouying758@126.com
Guodong Zhao: Network Management and Information Management Center, Ningxia University, Ningxia 750021, China, e-mail: zhaoguodong31@163.com
Roobaea Alroobaea: Department Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia, e-mail: r.robai@tu.edu.sa
Abdullah M. Baqasah: Department of Information Technology, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia, e-mail: a.baqasah@tu.edu.sa

distributed, large-scale, highly complex, and indirect development; this means that the network has higher requirements for security product technology, so people urgently need to study a new technology, in order to realize the perception and monitoring of large-scale network security situation [2]. There are some unique security issues in the large-scale and complex network environment, if it is difficult to achieve user data security and privacy protection, unable to plan and deploy security protection measures in a unified manner, and traditional security measures are difficult to meet the needs of massive information processing [3]. If you can grasp all kinds of security information in a large-scale and complex network environment in a comprehensive and timely manner, grasp the situation from the network as a whole, and evaluate and predict its development trend, can take effective measures to deal with various security threats, and improve system safety performance and self-protection capabilities. Figure 1 is a diagram of the network security situational awareness technology architecture.

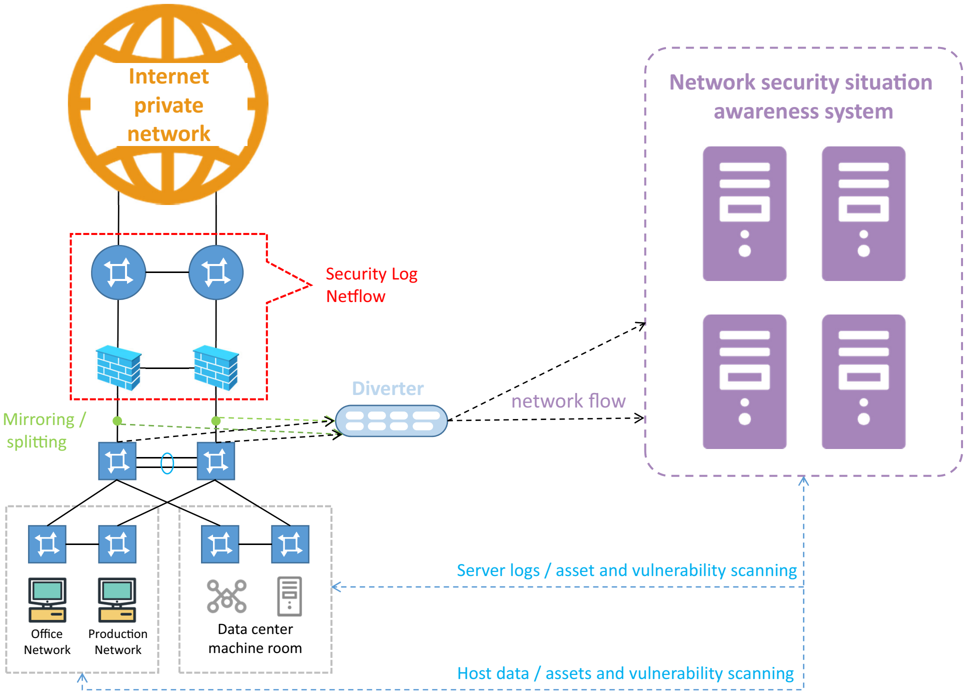

Figure 1: Network security situational awareness technology application architecture.

Network security situation awareness data come from various types of security systems; these systems provide different types of security events and data, and there is too much redundant information in these massive amounts of information, if directly used for safety assessment and prediction, will bring unnecessary trouble to data processing, and it also has a certain impact on the real-time performance of the processing results [4,5]. Therefore, data preprocessing must be performed on the original data set, and on this basis, perform integration operations such as reduction, merging, and integration. In other words, data fusion is one of the foundations of cyber security situational awareness; only after compressing and refining safety information data through data fusion technology, the results can be used as an important basis for security posture assessment and threat assessment. However, the data of network security situational awareness have the remarkable characteristics of massive, cross-domain, heterogeneous, and distributed; traditional network security situational awareness data fusion technology is applied to large-scale network environment, facing huge challenges and difficulties [4,6]. Network security situation awareness uses timely collection and processing of network security situation changes to provide the basis for the management of the network and improve the network security early warning ability.

Based on this study, a method for extracting information about the security situation of the network based on cloud computing has been developed. On the one hand, by combining the advantages of traditional feature selection methods and deep self-coding algorithms in the processing of large unlabeled samples; on the other hand, the advantages of cloud computing cannot be exploited in traditional algorithms for large-scale data processing. Alternatively, failures and performance verifications of the inability to efficiently process large amounts of data can be demonstrated through simulation tests to demonstrate the high performance of the method described in this document to improve knowledge of network security conditions.

2 Literature review

In a large-scale network environment, the network system is more complex; the diversity of users, the openness of services and systems have become the main features, making the traditional information security problem more serious. For the above reasons, researchers have begun research on cyber security situational awareness technology, mainly for real-time monitoring of the current network security situation, trying to find out some potential and malicious network behaviors as much as possible, before it has a bad impact on the network, a timely response strategy is given. Huang et al. proposed a network situation awareness model based on distributed multi-sensor data fusion; unfortunately, it failed to realize its prototype system. Subsequently, academia and research institutions based on their theoretical knowledge and models carried out relevant research in the field of network security situational awareness [7]. Fan et al. proposed a network security situation awareness method based on topology vulnerability analysis, use the extended finite state machine to determine all the states of the network, calculate the situational component values of threat existence, threat state, state transition probability, etc., so as to obtain network security situation information to realize network security situation awareness [5]. Zhang et al. proposed a situational awareness mechanism based on cognition, use self-organizing mapping to analyze the current network security situation and achieve visualization [1]. Radchikova and Odintzova et al. proposed a general network attack defense framework; it implements this defense framework by dynamically migrating server locations [8]. Mahlknecht et al. proposed that cyber security situational awareness is mainly divided into three stages: The awareness of network situation awareness, the understanding of network situation awareness, and the prediction of network situation awareness [9]. Meng and Wang et al. proposed to combine the advantages of situational awareness and network security technologies; it is helpful to enhance the management response ability of network managers to the current entire network [10]. Xi et al. used cognitive models to predict the network situation, and according to different defense models, it defines the overall level of network attack threats to network threats. To improve the robustness of the defense system through the overall detection of cyber threats, they designed a network situation decision support tool [11]. Liu et al. proposed a real-time defense system to conduct network security situational awareness. The system consists of distributed passive and active network sensors; the purpose is to effectively capture suspicious information related to cyber threats, develop an effective testing plan, and accurately distinguish between attack events and normal browsing time, in order to protect the security of the network [12]. Husak et al. proposed a hierarchical network security situational awareness model based on information fusion, and give the network security situation assessment workflow [13]. Jened et al. proceeded from the two perspectives of mobile collaborative perception platform and data fusion technology; by using the advantages of both the weighted average idea and the Kriging algorithm, the data fusion algorithm was successfully applied to the mobile collaborative perception platform [14].

The most important thing in the network security situation awareness is to collect and analyze the large-scale network security incidents, and to effectively describe the information, so that the network security managers can quickly grasp the network security situation. However, in practical application, network security situation perception is faced with many problems: (1) at the present stage, the network security alarm volume is large and the false alarm rate is high. When the data to be analyzed are large and continuous work, the network alarm volume can generally reach the order of G, among which about 90% of the alarm information is false alarm information. Therefore, how to dig out the useful information from the large-scale data is an important problem to be solved for the network security situation awareness; (2) the attack activities in the network will largely produce large-scale trivial alarm information, many types, the correlation is difficult to determine, and how to accurately identify the attack behavior as the problem to be solved by the security situation awareness. For the aforementioned problems, a network security situational awareness technology based on data mining is proposed.

3 Research methods

3.1 Cyber security situational awareness technology architecture

Network situation is the network operating status and changing trend composed of factors such as the working conditions of different network devices, network behaviors, and user behaviors. Network situation awareness is in a complex network environment, collecting security factors that can cause changes in the network situation, and predicting the future situation of the network. It integrates different types of perception data sources through big data technology, through data mining technology, convert different network security data that are out of order and seemingly unrelated into intuitive information, and complete network security situational awareness [15]. Therefore, this research uses the cloud computing platform to complete the collection and analysis of network security situation information; the frame structure is shown in Figure 2.

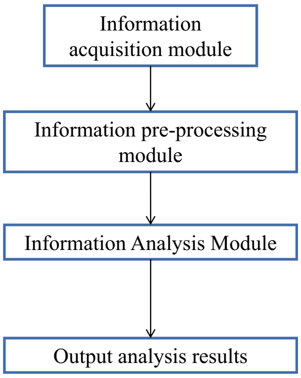
Information acquisition module
Information pre-processing module
Information Analysis Module
Output analysis results

Figure 2: Cloud computing platform framework.

Perceiving the network security situation, it mainly includes the following three important stages: the first stage is to collect different types of security data such as terminals, borders, and applications in the entire defense range, get data related to network security, at the same time, the data are stored uniformly, and a secure database is generated. The second stage uses data mining technology to discover security incidents, analyze potential threats, and predict unknown threats. The third stage is to estimate and perceive the network security situation based on data mining. The overall architecture is described in Figure 3.

3.2 Data collection

In the process of cyber security situational awareness, data are the basis of research, the choice of data type plays an important role in the final research results. Data collection consists of three parts, followed by

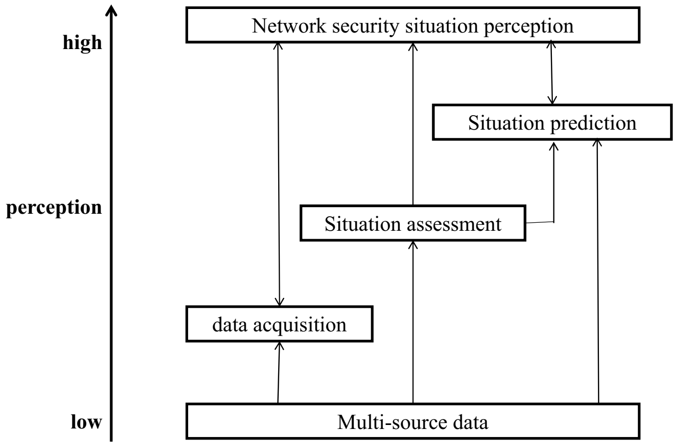

Figure 3: Network security situational awareness framework.

device log collection, sensor collection, and data preprocessing. The device log mainly collects log data generated by different security devices on the network; sensors can provide more complete data, improve the reliability of analysis results; preprocessing mainly preprocesses the collected data, delete some invalid data, so as to get more accurate analysis results [16,17]. Before preprocessing the data, transform every network security incident received into a standard format that can be processed; there are many types and large scales of network security events collected, but it can be described in the form of the following tuples as shown in formula (1):

$$W_i = [T_d, \mathrm{ET}, a_i, \mathrm{IP}_s, \mathrm{IP}_d, P_s, P_d, p_i, s_i, c_i, s_y, \text{other}], \tag{1}$$

where T_d is used to describe the time when a network security incident occurred, a_i is used to describe the level of network security events, ET is used to describe the types of network security events, IP_s and IP_d are used to describe the source and destination addresses of network security incidents, P_s and P_d are used to describe the source port and destination port of a network security event, p_i is used to describe the type of protocol, s_i is used to describe the sensor that collected the security event, c_i is used to describe the credibility of the occurrence of network security incidents, s_y is used to describe the severity of network security incidents, and other is used to describe the rest of the network security event information. There are differences in the sources of network security incidents, and there are also differences in the format of information collected; the event needs to be transformed into a unified form, in order to facilitate subsequent processing.

3.3 Network security situation assessment

3.3.1 Extraction of association rules based on data mining

Through data mining methods, conduct pattern mining, pattern analysis, and learning for network security event data sets; in order to complete the extraction of network security situation rules, it provides a basis for network security situation estimation. Assuming that W represents the collection of all project elements, it can be described as $W = \{w_1, w_2, \cdots, w_n\}$. Data set $R = \{r_1, r_2, \cdots, r_n\}$, among them, the element r_i of R is a set composed of elements in the set W, that is, $r_i \subseteq W$.

Definition 1. Set C is composed of elements in R, if the number of $C \subseteq r_i$ in the data set R is l, then the support of set C in data set R can be calculated by $\sup(C) = l/n$, if $\sup(C)$ exceeds the minimum support threshold ε, then the set C is the frequent k item sets of the data set R.

Definition 2. If the set C and D conform to $A \subseteq W \cap D \subseteq W$, then the confidence of $C \rightarrow D$ can be described as $\frac{\sup(C \cup D)}{\sup C}$. Association rules are mainly to mine the $C \rightarrow D$ that meets the minimum support and minimum confidence in the data set is based on the shopping basket problem; through the mining of frequent item sets of things, we can discover the association rules between things; this method has been widely used in many fields such as retail, finance, e-commerce, and so on.

Association rule mining mainly includes two steps: first, mine frequent item sets that meet the minimum support degree, the second is to mine the association rules that meet the minimum confidence level according to frequent item sets. In view of the large scale of network security situation data, mining association rules with the help of Hadoop platform [18]. Get a subset of the item set through the Map function, collect the support of all subsets in the instrument through the Reduce function, in order to obtain the support of frequent items, mining the frequent item sets in the data set, the detailed steps are as follows:

Input: the input path of the original network security data set R, the minimum support β.

Output: Frequent item set files meeting the minimum support degree.

(1) According to the path of the input file, from the minimum support frequent item sets file to the original network security data set, divide it into n data subsets of uniform size, format each row of the subset to form a <key, value> key-value pair, the key represents the character offset, and the value represents the data information. (2) Use the Map function to pair each <key in the subset, value> key-value pair to read, parse the value into the collection through the split function. (3) Treat all subsets as output keys, at the same time, assume that the value of each subset is 1. (4) Call the optional Combin function, in the massive network security data, all Map terminals will form large-scale key-value pairs with consistent key values, if all the obtained key-value pairs are transmitted to the Re-duce end using the network, the efficiency will be greatly reduced, therefore, use the Combin function to merge the same key-value pairs together.

3.3.2 Network security posture assessment

Cyber security posture is the distribution of the intrusion of the monitored network within a period of time and the impact on the security goal [19–26]. Network security situation information is mainly related to time and space, for an independent node, after it is attacked [27–34], both the attack index and resource impact will change [35–39]. Calculate the security risk level of the network node according to the alarm time after fusion, it is mainly related to the alarm confidence level c, the alarm severity level v, and the resource impact h [40–46]. The alarm confidence is calculated by using the initial definition and fusion, the alarm severity level is set, the degree of resource impact is related to network configuration and business [47–51]. In addition to the above analysis, it is also necessary to consider node security defense level e_n and alarm recovery coefficient s_n. The security situation assessment value of an independent node can be obtained by the following formula:

$$Z_n(t) = \sum c_i v_i h_i / e_n s_n. \tag{2}$$

In the process of evaluating the network security posture, we need to analyze the risks of different nodes in the network, because the position and role of nodes in the network are different, so the key level of nodes is also very different, therefore, the node weight ω_n needs to be calculated. The network security risk value can be calculated by the following formula:

$$Z_n(t) = \sum \omega_n Z_n(t). \tag{3}$$

In the above analysis, mainly analyze the network security alarm target node, but in practical applications, the complete security situation also needs to analyze the activity level of the intruder [52–55]. Therefore, it is also necessary to obtain the attack index of the intruder according to the network security alarm source address. The formula description is shown as follows:

$$Q_n(t) = \sum c_i v_i, \tag{4}$$

Through the above analysis, we can get the change curve of the network security situation assessment value over time, based on the estimated value of the network security situation; the prediction of the network security situation can be realized, complete the perception of the network security situation.

4 Results and discussion

4.1 Experimental data

The experimental window is 1 min, the data in the attack detection data set have about 1,000 time windows within 16 h, the experimental data time is 16 h in total, 39,125 pieces of data are obtained through one-way filtering, there were seven security incidents in the entire data set, there are three types of attacks, and the specific network security event information is described in Table 1.

Table 1: Security event table

Type	Time	Invaded party	Duration/s
U2R	8:24:11	168.12.115.50	241
R2L	8:55:34	168.12.110.50	2
PROBE	9:50:21	168.12.0.2	40
U2R	10:28:04	168.12.112.50	181
R2L	11:50:28	168.12.100.100	14
U2R	12:34:41	168.12.114.50	85
PROBE	21:24:12	168.12.1132.50	17

4.2 Experimental process and analysis

In the experimental environment, 168.12. XX stands for internal network, in order to get complete intrusion data, there was no defense when conducting the experiment, so when perceiving the network security situation, it also uses a method of manually changing the experimental data, after the experiment has been carried out for a certain period of time, simulate false positives, false negatives or when security defenses are in effect, changes in cyber security situational awareness, so as to verify the validity of the author's method [56]. Figures 4 and 5 adopt the method of this article; from the perspective of the original situation and artificial changes, the network security situational awareness attack index is calculated.

In Figure 4, the most primitive security threats are shown in the range of 0–500 windows, since the network has no security defense, all access from outside the network, small packets related to network security incidents enter the subnet so it can be reflected in the attack. After the 500th time window, defensive processing for network security incidents began.

Figure 5 shows that after manually reducing the 295th time window of network security incidents, using the obtained attack index, after discovering that the security incident was cancelled, the corresponding window attack index is reduced to 0, and it shows that the author's method can effectively realize network security situational awareness.

The above analysis is the author's perception of changes in the network security situation; the following analyzes the actual changes in the network security situation, described by the defense index, analyzes whether the author's method perception results are consistent with the actual network situation

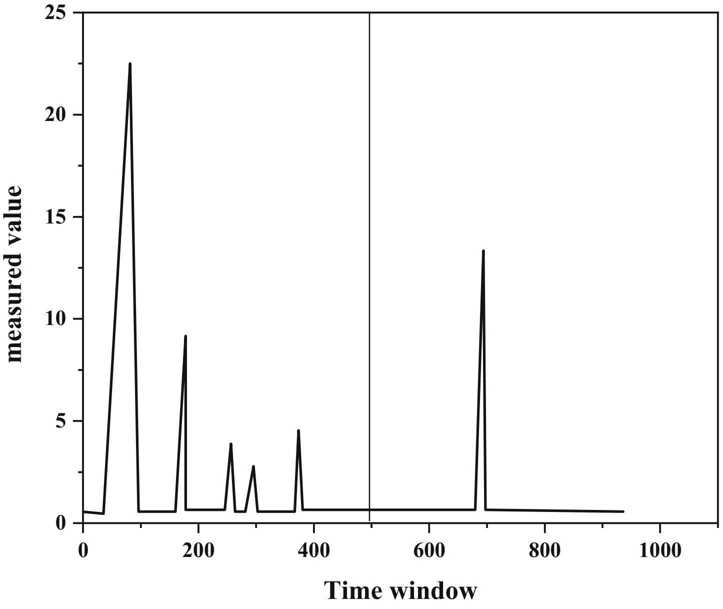

Figure 4: The original data attack index change graph.

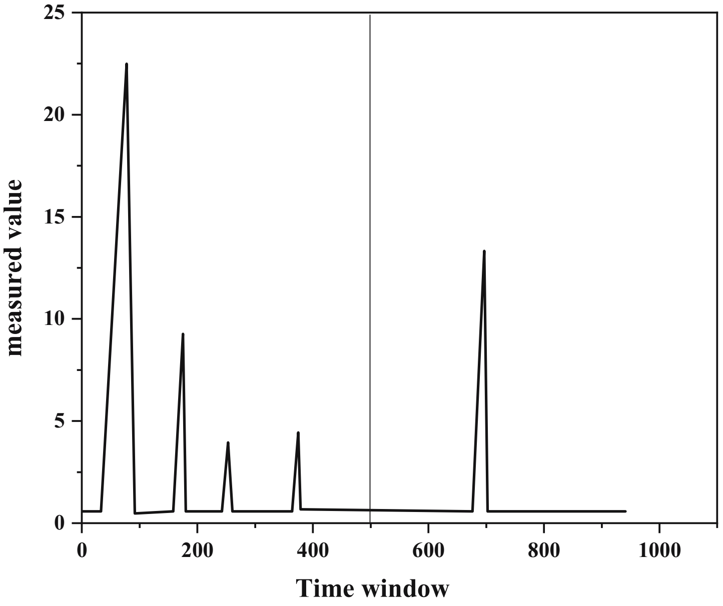

Figure 5: Changes in attack index after reducing scanning.

changes. In Figure 6, cyber security incidents have appeared since the 20th time window, after that, the defense index decreased, until the 500th window; this is mainly due to the lack of security defenses on the network during this period of time. At 500 windows, the defense index increased, which was consistent with the author's method perception result, explaining that the author's method can perceive changes in the network security situation.

In Figure 7, from the first window of attack, the defense index begins to decrease, in order to simulate the added cyber defense, reduced the 295th time window of cyber security incidents in the original data, during the corresponding period of time, the defense index increased significantly, consistent with the

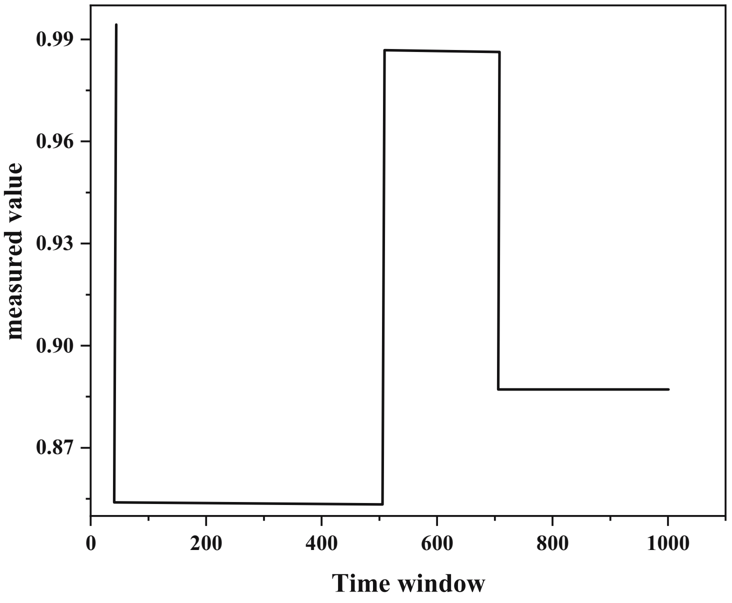

Figure 6: The original data defense changes.

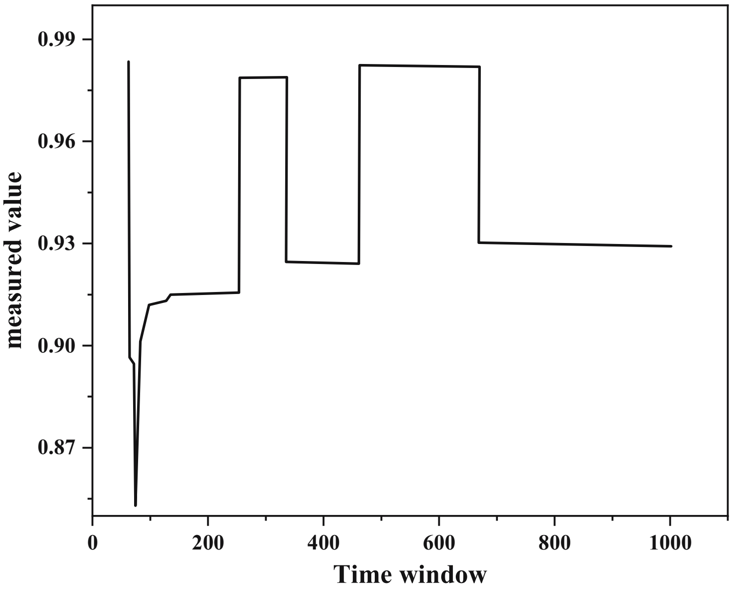

Figure 7: Simulation of the defense situation of network security incidents being intercepted.

author's method perception result, it further verifies the validity and reliability of the author's method for the perception of network security incidents.

5 Conclusions

With the rapid development of the network, the network scale continues to expand, and new network applications and technologies also continue to appear. Due to the openness and sharing of modern network systems, it leads to frequent attacks, rampant viral threats, and various major cyber security incidents.

In the face of continuous attacks and threats, various network security devices and defense systems are widely used. Although they improve the security of the network to a certain extent, various detection mechanisms also bring massive network traffic data, which cause some obstacles to the security situation awareness of network managers. Many research institutions began to try to overcome the difficulties of these massive information processing, and timely adjust the network security strategies and network management systems to meet the needs of large-scale networks. On the basis of constructing a network security situational awareness model, combining methods of steady-state feature analysis and safety information assessment, it can realize the optimal deployment design and security design of the security node of the hybrid structured network. The research on data mining method of network security situation awareness based on cloud computing is proposed.

The proposed method has the following advantages: (1) can provide simple and effective overall framework of network security situation perception, give basic ideas for related problems; (2) simplify the large-scale network security event database through data mining technology, obtain the network security situation association rules; (3) establish the network security situation model according to the correlation rules to estimate and predict the network security situation. The next step to be strengthened is as follows: (1) optimize the design of the technical structure under the existing framework, improve the perceptual performance of the larger scale network security situation; and (2) focus on the prediction methods of major network security events. Through data mining technology, effectively complete the simplified processing of the large-scale network security event database, obtain the association rules of the network security situation by mining frequent patterns. According to the association rules, establish a cyber security posture model, estimate and forecast the network security situation.

The next research work can be deeply studied from the following aspects:

(1) Improve the processing of network traffic data

With the emergence of large-scale complex networks, network security situation awareness data present new characteristics: massive, multi-source, and heterogeneous. This allows the system to produce different descriptive data for the same object in the real world, thus affecting the accuracy of network security situation perception results. Therefore, how to solve the problem of data inconsistency and conduct unified description and identification need further research and discussion of data.

(2) Realize the optimal selective integration classifier

When implementing the selective integration base classifier, it is a serial process to select the base classifier with large accuracy and then select the large difference, but there may be a base classifier with small accuracy but large difference to be removed; so how to integrate the base classifier by combining accuracy with difference will be further studied.

Funding information: This work was supported in part by the Project of Natural scientific Research Foundation of Ningxia, Grant No. 2021AAC03118. This work was supported in part by the Ideological demonstration course project of Tianjin Open University, Grant No. KCSZ202006.

Conflict of interest: Authors state no conflict of interest.

References

[1] Zhang D, He Q. Security situation awareness method for smart grid. Int Core J Eng. 2020;6(5):49–55.

[2] Jha RK, Puja, Kour H, Kumar M, Jain S. Layer based security in narrow band internet of things (NB-Iot). Computer Netw. 2020;185(3):107592.

[3] Ahmad I, Yau K, Ling MH, Keoh SL. Trust and reputation management for securing collaboration in 5g access networks: the road ahead. IEEE Access. 2020;8(99):62542–60.

[4] Lin P, Chen Y. Network security situation assessment based on text simhash in big data environment. Int J Netw Sec. 2019;21(4):699–708.

[5] Fan Z, Xiao Y, Nayak A, Tan C. An improved network security situation assessment approach in software defined networks. Peer-to-Peer Netw Appl. 2019;12(2):295–309.

[6] Han W, Tian Z, Huang Z, Zhong L, Jia Y. System architecture and key technologies of network security situation awareness system YHSAS. Computers Mater Continua. 2019;59(1):167–80.

[7] Huang F. Current situation and future security of agricultural water resources in north china. Strategic Study Chin Acad Eng. 2019;21(5):28–37.

[8] Radchikova NP, Odintzova MA. Assessment of the covid-19 pandemic situation: data from two countries with different security measures taken by authorities (Belarus and Russia). Data Brief. 2021;35(2):106917.

[9] Mahlknecht J, González-Bravo R, Loge FJ. Water-energy-food security: a nexus perspective of the current situation in Latin America and the Caribbean. Energy. 2020;194(Mar.1):116824.1–116824.17.

[10] Meng X, Wang X. 2018: international security order in vibration and reshaping. Contemporary World. 2019;22(1):18–22.

[11] Xi R, Yun X, Hao Z. Framework for risk assessment in cyber situational awareness. IET Inf Sec. 2019;13(2):149–56.

[12] Wu X, Liu S, Sun Y, An Y, Dong S, Liu G. Ecological security evaluation based on entropy matter-element model: a case study of Kunming city, Southwest China. Ecol Indic. 2019;102(Jul):469–78.

[13] Husak M, Komarkova J, Bou-Harb E, Celeda P. Survey of attack projection, prediction, and forecasting in cyber security. Commun Surv Tutorials IEEE. 2019;21(1):640–60.

[14] Jened R. Patent protection for a method of ratoon rice management in supporting food security. NTUT J Intellect Property Law Manag. 2019;8(1):66–92.

[15] MingtongLi. Research on the mechanism and influence factors of urban style building based on cloud computing logistics information. Clust Comput. 2019;22(6):13873–80.

[16] Samriya JK, Patel SC, Khurana M, Tiwari PK, Cheikhrouhou O. Intelligent SLA-aware VM allocation and energy minimization approach with EPO algorithm for cloud computing environment. Math Probl Eng. 2021;2021(6):1–13.

[17] Song D, Xiong F, Jingjing Z, Junchang W, Lin Z, Song D, et al. VM migration algorithm for the balance of energy resource across data centers in cloud computing. J China Univ Posts Telecommun. 2019;26(5):26–36.

[18] Tao L. Application of data mining in the analysis of martial arts athlete competition skills and tactics. J Healthc Eng. 2021;2021(4):1–6.

[19] Amhoud E-M, Chafii M, Nimr A, Fettweis G. OFDM with index modulation in orbital angular momentum multiplexed free space optical links. 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring); 2021. p. 1–5. doi: 10.1109/VTC2021-Spring51267.2021.9448928.

[20] Gill HS, Singh T, Kaur B, Gaba GS, Masud M, Baz M. A Metaheuristic approach to secure multimedia big data for IoT-based smart city applications. Wirel Commun Mob Comput. 2021;2021:1–10.

[21] Kumar A, Sehgal VK, Dhiman G, Vimal S, Sharma A, Park S. Mobile networks-on-chip mapping algorithms for optimization of latency and energy consumption. Mob Netw Appl. 2021;1–15.

[22] Boguszewicz C, Boguszewicz M, Iqbal Z, Khan S.A, Gaba G.S, Suresh A, Pervaiz B. The fourth industrial revolution and cyberspace's mental wellbeing: harnessing science and technology for humanity. Global foundation for cyber studies and research; 2021.

[23] Amhoud E, Othman GR, Jaouën Y. Concatenation of space-time coding and FEC for few-mode fiber systems. IEEE Photonics Technol Lett. 1 April1, 2017;29(7):603–6. doi: 10.1109/LPT.2017.2675919.

[24] Amhoud E-M, et al. Experimental demonstration of space-time coding for MDL mitigation in few-mode fiber transmission systems. 2017 European Conference on Optical Communication (ECOC); 2017. p. 1–3. doi: 10.1109/ECOC.2017.8345841.

[25] Gaba GS. Privacy-preserving authentication and key exchange mechanisms in internet of things applications. (Doctoral Dissertation). Lovely Professional University Punjab; 2021.

[26] Choudhary K, Gaba GS. Artificial intelligence and machine learning aided blockchain systems to address security vulnerabilities and threats in the industrial Internet of things. Intell Wirel Commun. 2021;329:454–65.

[27] Zerhouni K, Amhoud EM, Chafii M. Filtered multicarrier waveforms classification: a deep learning-based approach. IEEE Access. 2021;9:69426–38.

[28] Gaba GS, Kumar G, Monga H, Kim TH, Liyanage M, Kumar P. Robust and lightweight key exchange (LKE) protocol for industry 4.0. IEEE Access. 2020;8:132808–24.

[29] Sharma A, Kumar N. Third eye: an intelligent and secure route planning scheme for critical services provisions in internet of vehicles environment. IEEE Syst J. 2021;16(1):1217–27.

[30] Kumar P, Gaba GS. Biometric-based robust access control model for industrial internet of things applications. IoT Sec Adv Authent. 2020;133–42.

[31] Hedabou M. Cryptography for addressing cloud computing security, privacy and trust issues. Book on computer and cyber security: principles, algorithm, applications and perspective. USA: CRC Press, Francis and Taylor Publisher; 2018.

[32] Iggaramen Z, Hedabou M. FADETPM: Novel approach of file assured deletion based on trusted platform module. In lecture notes in networks and systems. vol. 49, Rabat, Morocco: Springer Verlag; 2017. p. 49–59.

[33] Azougaghe A, Hedabou M, Belkasmi M. An electronic voting system based on homomorphic encryption and prime numbers. In International Conference On Information Assurance and Security. Marrakech; 2015.

[34] Bentajer A, Hedabou M, Abouelmehdi K, Igarramen Z, Fezazi S.E. An IBE-based design for assured deletion in cloud storage. Cryptologia. 2019;43(3):254–65. doi: 10.1080/01611194.2018.1549123.

[35] Gaba GS, Kumar G, Monga H, Kim TH, Kumar P. Robust and lightweight mutual authentication scheme in distributed smart environments. IEEE Access. 2020;8:69722–33.

[36] Hedabou M. Some Ways to secure elliptic curves cryptosystems. J Adv Cliford Algebras. 2008;18:677–88.

[37] Gaba GS, Kumar G, Kim TH, Monga H, Kumar P. Secure device-to-device communications for 5g enabled internet of things applications. Computer Commun. 2021;169:114–28.

[38] Sharma A, Podoplelova E, Shapovalov G, Tselykh A, Tselykh A. Sustainable smart cities: convergence of artificial intelligence and blockchain. Sustainability. 2021;13(23):13076.

[39] Bentajer A, Hedabou M, Abouelmehdi K, Elfezazi S. CS-IBE: a data confidentiality system in public cloud storage system. Procedia computer science. vol 141. Leuven, Belgium: Elsevier; 2018. p. 559–64.

[40] Azougaghe A, Hedabou M, Oualhaj O, Belkasmi M, Kobbane A. Many-to -One matching game towards secure virtual machine migrating in cloud computing. International Conference on Advanced Communication System and Information Security. Marrakech; 2016.

[41] Masud M, Gaba GS, Choudhary K, Hossain MS, Alhamid MF, Muhammad G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet Things J. 2021;9(4):2649–56.

[42] Sharma A, Singh PK, Sharma A, Kumar R. An efficient architecture for the accurate detection and monitoring of an event through the sky. Computer Commun. 2019;148:115–28.

[43] Masud M, Gaba GS, Choudhary K, Alroobaea R, Hossain MS. A robust and lightweight secure access scheme for cloud based E-healthcare services. Peer-to-peer Netw Appl. 2021;14(5):3043–57.

[44] Hedabou M, Frobenius A. Map Approach for an Efficient and Secure Multiplication on Koblitz curves. Int J Netw Security. 2006;3(2):233–7.

[45] Sharma A, Georgi M, Tregubenko M, Tselykh A, Tselykh A. Enabling smart agriculture by implementing artificial intelligence and embedded sensing. Computers Ind Eng. 2022;165:107936.

[46] Boukhriss H, Hedabou M, Azougaghe A. New technique of localization a targeted virtual. In Proceedings of the 5th International Workshop on Codes, Cryptography and Communication Systems, El Jadida November 27–28; 2014.

[47] Suo N, Zhou Z. Computer assistance analysis of power grid relay protection based on data mining. Comput Des Appl. 2021;18(S4):61–71.

[48] Bardak S, Bardak T, Peker H, Szen E, Abuk Y. Predicting effects of selected impregnation processes on the observed bending strength of wood, with use of data mining models. Bioresources. 2021;16(3):4891–904.

[49] Wu B, Qin D, Hu J, Liu Y. Experimental data mining research on factors influencing friction coefficient of wet clutch. J Tribol. 2021;143(12):1–14.

[50] Wang B. Multimedia filtering analysis of massive information combined with data mining algorithms. Adv Multimed. 2021;2021(3):1–7.

[51] Chauhan S, Miglani R, Kansal L, Gaba GS, Masud M. Performance analysis and enhancement of free space optical links for developing state-of-the-art smart city framework. Photonics. 2020;7:132. doi: 10.3390/photonics7040132.

[52] Xu H, Li X. Methods for virtual machine scheduling with uncertain execution times in cloud computing. Int J Mach Learn Cybern. 2019;10(2):325–35.

[53] Sreenu K, Sreelatha M. W-scheduler: whale optimization for task scheduling in cloud computing. Clust Comput. 2019;22(6):1–12.

[54] Mss A, Pmjp B. Nature inspired chaotic squirrel search algorithm (CSSA) for multi objective task scheduling in an IaaS cloud computing atmosphere - sciencedirect. Eng Sci Technol Int J. 2020;23(4):891–902.

[55] Singhal R, Singhal A. A feedback-based combinatorial fair economical double auction resource allocation model for cloud computing. Future Gener Computer Syst. 2021;115(2S6):780–97.

[56] Jagota V, Luthra M, Bhola J, Sharma A, Shabaz M. A secure energy-aware game theory (SEGaT) mechanism for coordination in WSANs. Int J Swarm Intell Res (IJSIR). 2022;13(2):1–16.