
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2023 SCPE. Volume 24, Issues 4, pp. 663–672, DOI 10.12694/scpe.v24i4.2069

SECURE STORAGE OF COMPUTER NETWORK DATA BASED ON CLOUD COMPUTING

HONGWEI JIANG*

Abstract. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. User's data is stored in large database. The stored data can be accessed and modified by the clients over the Internet. The data is monitored by the Third Party Auditor (TPA) on behalf of the client. Therefore, integrity is lacked by the data stored on the servers. The data integrity is ensured by the cloud services that provide trust to the privacy of users. Aiming at the urgent problem of network data security in cloud computing operations, this paper proposed a security situation assessment system to grasp the security situation in real time. A set of cloud computing network data storage security is proposed. Through this model, the extraction of network data storage security situation elements, the design of network data storage security situation assessment scheme and the calculation method of network data storage security situation value are completed. The experimental results show the error of the predicted value obtained by the network data storage security situation assessment system. The effectiveness of the system model and the superiority of the improved algorithm is verified by the experimental results. This paper uses the cloud model to predict the cloud computing network security situation. On the other hand, the security situation value obtained by the situation assessment process can be used directly without training the original situation value. Performance improvement by the proposed technique over existing technique is seen and it is observe that the proposed technique is 23% and 34% better than the existing techniques.

Key words: Cloud computing; Network security; Situational assessment; Situational prediction; Secure storage; Third Party Auditor; Computing resources

1. Introduction. The cloud storage system's development and its application in complex environment are increasing rapidly, so, the security of the data has been more and more consideration. With the birth of computers and the rapid development of the Internet, the current research focus is to combine computers that run alone to deal with problems, improve processing power and processing efficiency, and achieve effects similar to "supercomputers". Cloud computing is one of the most popular research directions in the current field. As a new type of network architecture and network computing model, all sectors of society have paid special attention. The improvement of cloud computing service technology to realize multi-tenant technology ensures that they can have some customized functions. The Internet is the carrier for cloud computing to realize resource sharing. However, the Internet also has heterogeneity and openness. Therefore, cloud computing operations may be attacked by the network all the time, such as malicious tampering of user information, interception or deletion of user data, etc. It can be seen that in the cloud computing system, safe and effective network protection and monitoring are very necessary for the entire security system. The research on network security management based on cloud computing is shown in Figure 1.1.

Another important function of the cloud computing platform is data storage. Because the cloud computing platform stores a large amount of data of each node, and the services of the cloud computing platform are open and extensive, the cloud computing platform is subject to considerable attacks and harms. It is required to carry out the necessary security protection while the data is stored. To sum up, for the cloud computing platform, we need to formulate corresponding security protection assessment strategies, monitor the security status of the entire cloud computing system in real time, and provide detailed security protection logs. The entire platform is analyzed as a whole, resulting in a final analysis report. In this way, the combination of intelligent analysis platform and manual analysis can timely and accurately detect network attacks and make relevant security policy adjustments.

The great convenience is offered by moving huge data into cloud since it reduces hardware management

*Jilin Sport University, Jilin, Changchun, 130022, China (hongweijiang4321@yahoo.com).

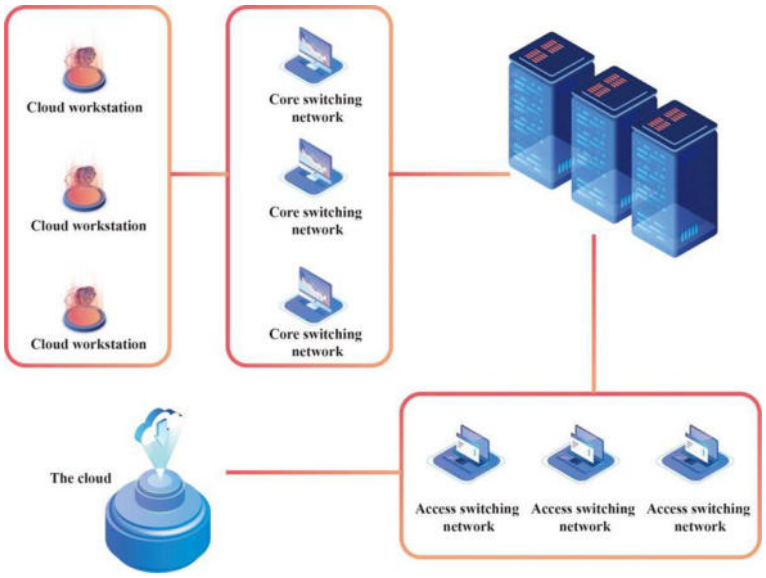

Fig. 1.1: Research on network security and management application based on cloud computing

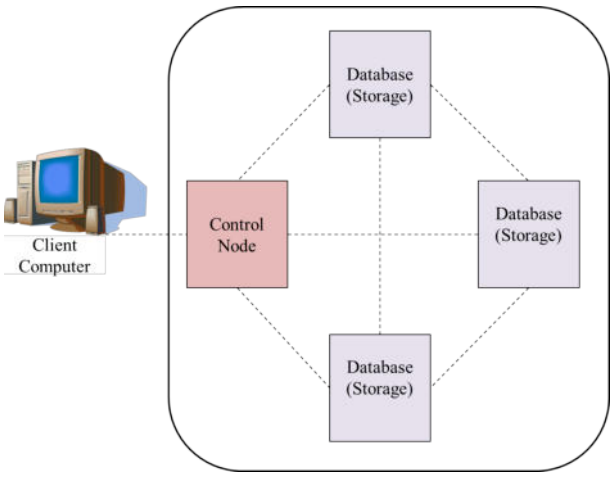

Fig. 1.2: Architecture of cloud storage system

and data maintenance burden. Many types of services such as data as a service and infrastructure are provided to users. Scalable, secure, for clients at low cost is offered by it. The CSP could discard the data which has not been accessed so to overcome the security threats, CSP require a mechanism for the users' data integrity insurance. The third party auditing is emerged to resolve the problem. A cloud storage system architecture includes a control server and storage servers, as shown in figure 1.2.

1.1. Contribution. 1. A research idea of adopting security situation assessment to grasp the security situation of the overall system in real time is presented.

2. The great convenience to users is offered by moving huge data into cloud since it reduces hardware management and data maintenance burden at local machines. Many types of services such as data as a service and infrastructure are provided to users. The third party auditing is emerged to resolve the problem.

Rest of the paper is organized as follows. The related work is reviewed and discussed in Section II followed

by the section III which explains the research methodology utilized in this work. Section IV gives the result analysis and Section V concludes the paper.

2. Literature Review. With the rapid development of cloud computing technology, there are several problems that need to be solved urgently, such as: cloud security problems are becoming more and more prominent, showing a diversified and complex trend, what security technology is used to protect the tenant's environment, etc. [1]. The research results of the Cloud Security Alliance listed in Literature [2] show that Internet-based cloud computing servers have been attacked by a large number of hackers. attack. Literature [3] pointed out that the concept of cloud computing originated from European and American countries. As the birthplace of this technology, they have mastered many leading theories and technologies, and as a result, many very famous companies in the field of cloud computing have emerged, such as Yahoo, Yahoo! Technology companies such as Microsoft and Google. In the literature [4], many operators around the world have also launched cloud computing-based services, such as BT in the UK and Verizon in the United States.

These countries have started to conduct research on network security in cloud computing very early, and the current technical level is in the leading position in the world. Taking the United States as an example, it already has a complete security infrastructure, security assessment criteria, certified encryption standards and related regulations, and has formed a sound information security industry chain [5]. Literature [6] pointed out that "Cloud Security Alliance" is a non-profit, non-profit organization, its task is to solve the security problems existing in the cloud computing network, propose solutions, and improve the security index of cloud computing. After the Cloud Security Alliance was established in the United States, cloud computing providers such as Microsoft and Google have joined the alliance. The alliance currently consists of 34 members. Reference [7] pointed out that the research in the field of cloud computing security in the United States has always been at the forefront of the world. American researchers have proposed a variety of cloud security frameworks, and many methods have been applied to actual cloud computing, such as: user data Encryption techniques, secure network connections, secure computers, etc. The giants of cloud computing service providers in the world have already formed an independent system in cloud security, such as increasing investment in cloud computing, attaching importance to research on cloud computing security, continuously strengthening their cloud computing platforms, and launching new cloud computing platforms. security mechanism, etc. [8].

Cloud computing technology started late in China and has not yet been applied on a large scale. Document [9] records the details of a research report called "Cloud Computing in China", which reflects the development of cloud computing in China well, and is a good example for the further development and innovation of cloud computing in China. Reference is provided. Literature [10] shows that, in order to promote the development of cloud computing, the government has established cloud computing R and D centers in Guangzhou, Shanghai, Beijing and other places, and actively conducts research on cloud computing-based applications and cloud computing security. In addition, many Internet companies have also joined the research team of cloud computing [11]. According to the analysis, the current research on the security situation assessment strategy of the cloud computing platform is still lacking and formulate the network security situation assessment of cloud computing platform [12].

The author in this paper detailed the cloud computing based computing model to support the shared pool of computing resources access. Due to the data outsourcing, integrity and data security, it becomes challenging [13]. Author in this paper discussed the process of fighting against network security and the traditional defense has been difficult. To meet the computer network security needs under cloud computing and for the cloud computing high-quality system can be optimized gradually. In this paper, the cloud computing is utilized for security storage design and to ensure the reliability and data upload storage security [14]. Program utilizes the boot password for the existing data encryption security in the management; system design by correcting Tornado data redundancy code. A secure cloud storage prototype system is also implemented by the author based on Cassandra. It is observe that the system can provide the ability of data loss recovery and effectively resist the fault [15]. The author in this article discussed the accessibility of the resources obtainable from the cloud whenever users want, therefore, users purchase the IT service that they do not have maintain things. The data storage model is computing which considers as a web-based generation which utilizes remote servers. Author gives new designing for the information security storage construction where information encrypted and divided into many blocks and distributed between services suppliers instead of relying on one supplier for

information storage [16].

Author in this paper discussed a new method of cloud computing that has brought great convenience to network life, but with some security risks. The concept and characteristics of cloud computing are described analyzes the significance for the computer network security in the cloud computing environment and analyzes the security vulnerabilities according to the cloud computing characteristics [17]. Author in this paper discussed a new method of cloud computing that has brought great convenience to network life, but with some security risks. Author in this paper presented a neuro-fuzzy approach for the user behaviour classification and prediction. The analysis is complicated by each user's feedback and the various rules have been implemented for addressing the company's policy to determine the precise behaviour of a user [18]. A Gaussian Radial Basis Function Neural Network (GRBF-NN) is trained for prediction on the basis of set generated by a Fuzzy Rule Based System (FRBS). The scheme is found to be promising in prediction accuracy. Author presented a resource-based task algorithm which is implemented and analyzed to understand the heterogeneous multi-cloud network performance [19]. Author in this paper, a heterogeneous integrated network resource management algorithm is presented. The algorithm adopts the information security transmission technology advantage to collect resources in heterogeneous integrated network and establishes a resource management algorithm model on the basis of information security transmission [20]. The resource management algorithm effectiveness is determined which reduces resource management errors and improve security performance in the resource management process. The main data encryption technology and intelligent collection process of the Internet of Things (IoT) is also discussed by the author. Author in this paper presented a new Chinese Remainder Theorem (CRT)-based data storage mechanism for the user data storage [21]. The CRT-based secured storage scheme adopts encryption schemes which use formulas for performing the encryption and also introduced a new formula for data decryption. In addition, a new formula is introduced for accessing the encrypted cloud data from the cloud database. The security models have been evaluated by analyzing the results and finally, it is proven that the proposed data security model is better comparatively. The author aims to develop a basic cloud-based design for ICC laboratories improvement. The proposed design is built via using "Software as a Service" model [22]. Cloud computing is designed by utilizing the Private Cloud Computing. The presented design provided flexibility to ICC and allows computer network capabilities improvement and managing the resources easily.

2.1. Problem Statement. User's data is archieved in large data centers. The stored data can be accessed and modified by the clients. The data is monitored by the Third Party Auditor on behalf of the client. Therefore, integrity is lacked by the data stored on the servers. The data integrity is ensured by the cloud services that provide trust to the privacy of users.

3. Proposed Method. The role of network security posture assessment in this paper is to inform the system of what dangers may occur, so as to realize the safe storage of network data. The specific process is to preprocess the collected original safety data information, extract the characteristic information of system safety events, and obtain an estimated probability value by using certain mathematical models and calculation methods to determine whether certain safety events occur. As shown in Figure 3.1, this model mainly has three layers from high to low: situational prediction, situational assessment and situational awareness.

The first layer is the situational awareness layer, which is the basis of the entire situational assessment model. At present, there are very mature technical means, which can obtain enough data through the situational awareness layer. By processing the collected data, all information about the current network operating status can be obtained. In order to complete the assessment of the security situation, the situation information is usually transformed into a form that is easier for people to understand, such as XML [23]. The second layer is the situation assessment layer, which is the core of the entire situation assessment model. Security identification is performed on the data obtained by the upper layer, the correlation between security events is mined, the security situation value is calculated, and a security situation curve graph is generated to reflect the security situation of the entire system. The third layer is the situation prediction layer, which judges and predicts the future security situation according to the past and present network security situation, and makes early response strategies and processing method. A significant feature of cloud computing is big data. A large amount of network data is a must for security situation assessment. Moreover, the redundancy between data and false information make the calculation method of situation assessment very complicated. Security situation assessment is a comprehensive research topic, which includes data processing methods, network modeling requirements, and so

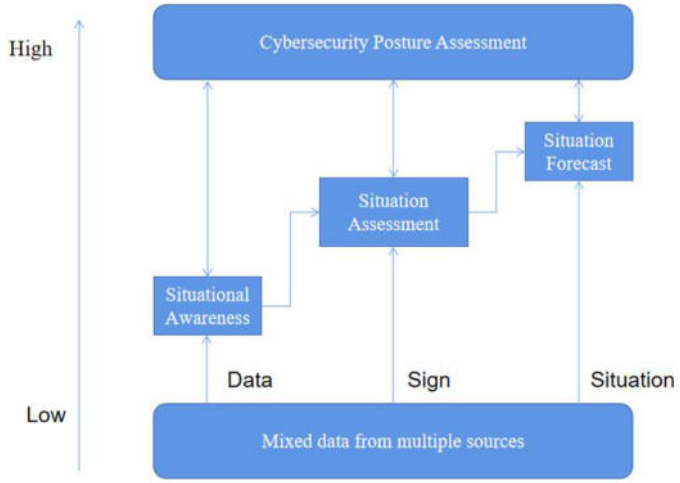

Fig. 3.1: Basic Model of Network Security Situation Assessment

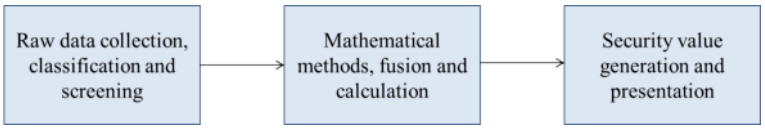

Fig. 3.2: The generation process of network security situation value

on. In the current technology and theory, the two major technologies of data mining and data fusion are the main methods for processing large amounts of data.

3.1. Calculation of security situation value. The size of the network security situation value can clearly characterize the operation of the network. The larger the situation value, the more unstable and dangerous the network operation is. After a series of mathematical calculations, after preprocessing the collected network data, the data is converted into one or several groups of data to obtain the network security situation value. The size of the network security situation value will change with the different network operating conditions. For example, the network has been attacked and suffered different types of attacks. By observing the changes in data, network security managers can judge the security situation of the network, and then judge whether the network is threatened. Figure 3.2 shows the process of generating a network security situation value.

This algorithm not only reduces the complexity of the original mapping algorithm, but also reduces the generated errors by using the super entropy value, which are all in the original mapping. Algorithms based on increased accuracy. During the solution process, the membership degree of each network security situation value is not used, but the cloud model parameters are calculated directly by using the statistical characteristics of the cloud model, which not only avoids certain errors, but also simplifies the mapping algorithm.

3.2. Challenges and Issues of Cloud Data Storage. The control over the stored data is not provided by the cloud computing based on cloud data centers. There is full data control by cloud service providers as they perform malicious tasks like copy, modifying, etc. The certain levels of control are ensured by the cloud computing over the virtual machines. Due to lack of control over the data, a greater security issues are there than the generic cloud computing model. The figure 3.2 has many issues which need to discuss clearly.

Less cost and less resource management is provided by the cloud computing but it has also some security threats. The cloud computing ensures the integrity, privacy and availability of data in cloud computing but it

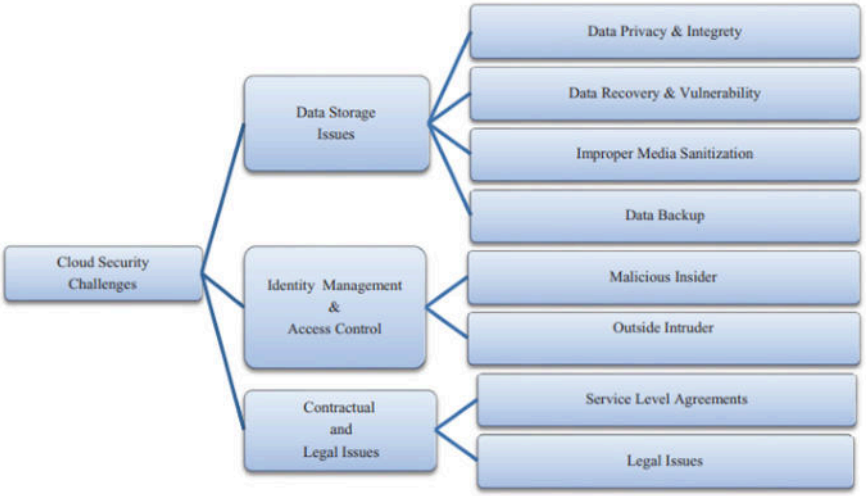

Fig. 3.3: Challenges of cloud security

Table 4.1: Attack Category and Threat Level

Attack Category	Level of threat
Misc_antivity	1
Network scan	1
RPC_port map decode	2
Attempted dos	2
Mapping modified	2
Attempted admin	3
Http_uri decode	3
Shell code detect	3

is vulnerable for the security threats. The simplicity cloud users are increasing and the applications hosted in cloud is very great.

4. Analysis of results.

4.1. Source of experimental data. At present, there are mainly three kinds of experimental data widely used in the assessment and prediction of network information security situation in the world: the honeynet data set collected by the honeynet project group of the network security organization; the Defcon data set provided by the network security expert organization ShmooGroup; and the MIT Lincoln experiment Lincoln Laboratory public dataset provided by the laboratory. According to the overview and characteristic analysis of the three data sets in the literature, the honeynet data set is very beneficial to be used as experimental data for simulation tests to simulate the data that may be generated when the cloud computing network system is attacked. This paper first uses honeynet data as the experimental test data, selects the honeynet data set of a certain month, and effectively combines the relevant knowledge of the open source intrusion detection system Snort, and summarizes the data set required for the experiment. The types of attacks on the network system used in the experiment are shown in Table 4.1, and the corresponding threat levels are also marked.

Table 4.2: The number of times the network was attacked

Type	Time 1	Time 2	Time 3	Time 4	Time 5	Time 6	Time 7	Time 8
Ping	40	0	1	0	8	50	45	0
DNS	3	9	6	24	14	35	24	10
DOS	0	16	1	0	20	20	10	5
RPC	0	6	1	0	0	10	5	3
Shellcode	2	4	0	0	1	3	1	0
Http	2	0	28	0	0	15	15	14

Table 4.3: The number of hosts attacked on the network

Type	Host number 1	Host number 2	Host number 3	Host number 4	Host number 5	Host number 6	Host number 7	Host number 8
Ping	1	0	1	0	1	1	1	0
DNS	1	3	1	6	2	8	3	4
DOS	0	5	1	0	8	6	5	3
RPC	0	3	1	0	0	5	5	2
Shellcode	1	2	0	0	1	3	1	0
Http	1	0	1	0	0	1	1	1

4.1.1. Analysis of experimental results. Combined with Table 4. 1, the experimental data is analyzed. This paper counts the attack elements, the number of attacks, and the number of attacked hosts on the network system in an average of 8 time periods within a month. The time can be determined according to the performance of the system. to resize. The statistical results are shown in Tables 4. 2 and 4. 3 below. The threat levels corresponding to the attack types Ping, DNS, DOS, RPC, Shellcode, and Http are 1, 2, 2, 2, 3, and 3, respectively.

According to Table 4.2 and Table 4. 3, it can be obtained that the security situation values of the network system in 1 month and 8 time periods (t1 t8) are (0.193, 0.214, 0.423, 0.076, 0.763, 0.872, 0.825, 0.565) respectively. The corresponding network The security situation diagram is shown in Figure 4.1.

It can be seen from Figure 4.1 that the security situation index value of the network system in the three time periods of t1, t2 and t4 is small, indicating that the network in this time period is in a relatively safe and stable state; the network is in a relatively safe and stable state at t3 , t5, t8, although it suffered a certain attack threat during the three time periods, but it can still operate normally; the security situation index of the network in the two time periods of t6 and t7 is high, indicating that the network in this time period suffered from When there is a serious attack threat and the network is in an unsafe state, network managers should pay more attention and take appropriate measures.

Comparing Tables 2 and 3, it effectively proves the rationality of the cloud computing network security situation assessment method designed in this paper, and the obtained assessment results conform to the objective facts. In the experiment, the data set is used to further verify the evaluation model and prediction algorithm designed in this paper. When the network security situation index value is between (0, 0.3), the network is running safely; when it is between (0.3, 0.8), the network has suffered a certain attack, but it can still operate normally; between (0.8, 1) When the network is in an insecure state, it has suffered a serious attack threat. Of course, in the actual security management process, network managers can dynamically set the threshold of the network security situation index according to specific security defense regulations. According to the cloud computing network security situation forecast introduced above, the predicted value of network security situation is obtained as shown in Figure 4.2. The figure shows the comparison between the predicted curve of network security situation and the actual curve, and the prediction of network security situation value in the next two weeks is drawn. value and true value. It can be seen from the figure that the trend of the predicted

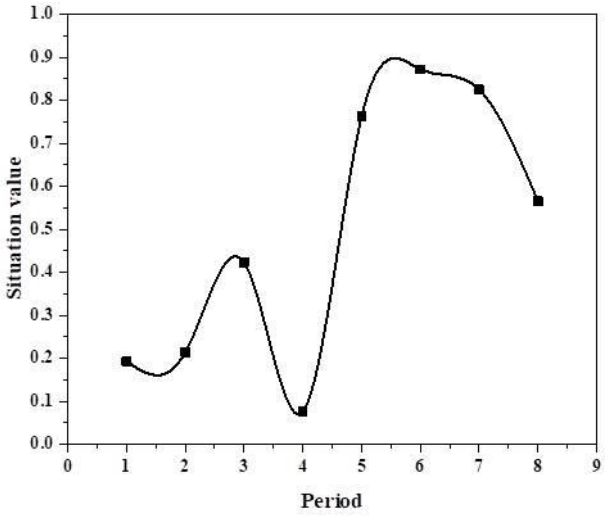

Fig. 4.1: Network Security Situation Map

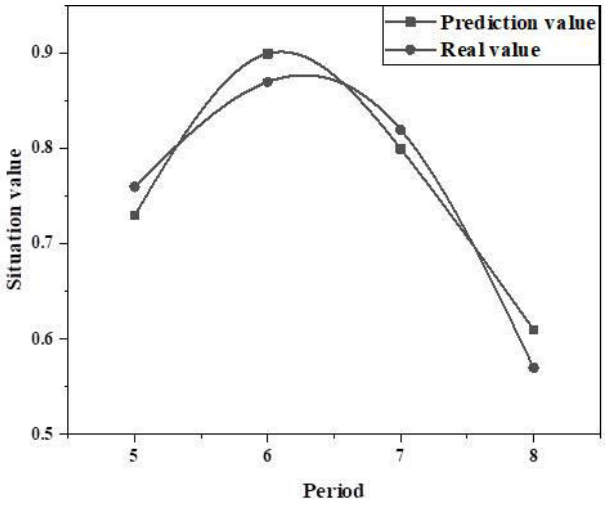

Fig. 4.2: Network Security Situation Forecast

curve and the actual curve have a trend value error of no more than 0.05 in the four time intervals, which is basically the same. This result shows that the improved network security situation prediction method adopted in this experiment is correct and meets the actual requirements.

The proposed technique performance is compared with the existing techniques in terms of prediction accuracy. It is better than the existing techniques in prediction accuracy. Performance improvement by the proposed technique over existing technique is shown graphically in Figure 4.3. It is seen that the proposed technique is 23% and 34% better than the existing and existing techniques.

5. Conclusion. After full analysis and the existing research knowledge, this paper firstly proposes an extraction model of network security situation elements according to the cloud computing architecture. The model is divided into three layers. And use the mapping algorithm based on this model to calculate the network security situation value. Secondly, in view of the randomness and ambiguity of the network state, this paper uses the cloud model to predict the cloud computing network security situation. Finally, the prediction results

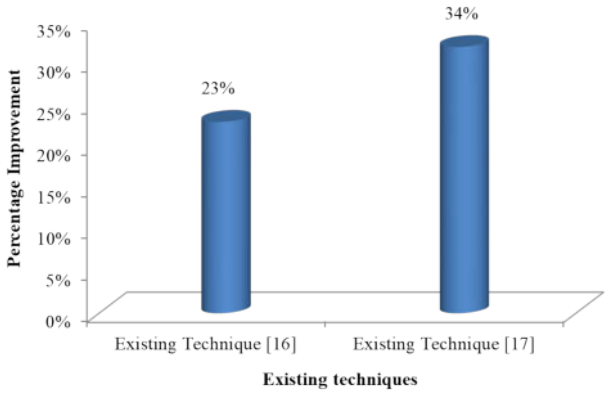

Fig. 4.3: Performance Improvement of the proposed technique over existing techniques

of network security situation are presented in tabular and graphical forms respectively, which verifies the correctness and superiority of the mapping algorithm and the element model of network security situation.Compared with the traditional network security situation assessment research, there are few related researches on cloud computing and the research in this paper is not very complete and comprehensive. It is hoped that the future research directions are: 1. According to the characteristics of cloud computing big data, Investigate better algorithms so that data can be analyzed from the data that is more useful for cloud security. 2. For the specific environment of cloud computing, further study the security situation assessment algorithm and the security situation prediction algorithm to make the assessment results and prediction results more accurate and more in line with the objective reality. 3. Strive to design and develop a software system, which is truly used for cloud computing network security situation assessment, and can realize automatic control and real-time update. Performance improvement by the proposed technique over existing technique is seen and it is observe that the proposed technique is 23% and 34% better than the existing techniques.

REFERENCES

[1] Novo, O. Ding, M. H., Research on Clustering Algorithm of Heterogeneous Network Privacy Big Data Set Based on Cloud Computing, International Conference on Advanced Hybrid Information Processing (pp. 367-376). Springer, Cham, 2021.
[2] Liu, Y., International logistics taxation data monitoring based on 5g network and cloud computing platform, Microprocessors and Microsystems, 82, 103826, 2021.
[3] Gong, J. , Design of Distributed Network Mass Data Processing System based on Cloud Computing Technology, 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021.
[4] Song, H. , Li, J. , & Li, H. , A cloud secure storage mechanism based on data dispersion and encryption, IEEE Access, 9, 63745-63751, 2011.
[5] Khalaf, O. I. , & Abdulsahib, G. M., Optimized dynamic storage of data (odsd) in iot based on blockchain for wireless sensor networks, Peer-to-Peer Networking and Applications, 1-16, 2021.
[6] Kim, M. , Jiang, X. , Lauter, K. , Ismayilzada, E. , & Shams, S., Hear: human action recognition via neural networks on homomorphically encrypted data, arXiv preprint arXiv:2104.09164, 2021.
[7] Zhong, C. , Jiang, X. , & Qi, G., Video-based person re-identification based on distributed cloud computing, Journal of Artificial Intelligence Technology(2), 11, 2021.
[8] Zhang, L., Optimization of the marketing management system based on cloud computing and big data, Complexity, 2021.
[9] Kahn, M. G. , Mui, J. Y. , Ames, M. J. , Yamsani, A. . , Pozdeyev, N. , & Rafaels, N., Migrating a research data warehouse to a public cloud: challenges and opportunities, Journal of the American Medical Informatics Association, 2021.
[10] Dehury, C. K. , & Sahoo, P. K., Failure aware semi-centralized virtual network embedding in cloud computing fat-tree data center networks,arXiv e-prints, 2021.
[11] Tian, J. , & Wang, H., A provably secure and public auditing protocol based on the bell triangle for cloud data, Computer Networks, 195(1), 108223, 2021.
[12] Susilo, W. , Jiang, P. , Lai, J. , F.Guo, & Deng, R., Sanitizable access control system for secure cloud storage against malicious data publishers, IEEE Transactions on Dependable and Secure Computing, PP(99), 1-1, 2021.

[13] Subashini, S., & Kavitha, V., A survey on security issues in service delivery models of cloud computing, Journal of network and computer applications, 34(1), 1-11, 2011.
[14] Wang, X., & Shi, L. Design of computer network security storage system based on cloud computing technology. In Journal of Physics: Conference Series (Vol. 2083, No. 4, p. 042084). IOP Publishing, 2021.
[15] Wang, R. Research on data security technology based on cloud storage. Procedia engineering, 174, 1340-1355, 2017.
[16] Kadhim, Q. K., Mahdi, H. S., & Ail, H. K., Storage Architecture for Network Security in Cloud Computing. Diyala Journal for Pure Science, 14(1), 1-17, 2018.
[17] Luo, L., & Ge, W. Research on the Security of Computer Network under Cloud Computing. In 2018 3rd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2018) (pp. 278-281). Atlantis Press, 2018.
[18] Dash, S., Luhach, A. K., Chilamkurti, N., Baek, S., & Nam, Y. A Neuro-fuzzy approach for user behaviour classification and prediction. Journal of Cloud Computing, 8(1), 17, 2019.
[19] Mishra, S. K., Mishra, S., Alsayat, A., Jhanjhi, N. Z., Humayun, M., Sahoo, K. S., & Luhach, A. K. Energy-Aware Task Allocation for Multi-Cloud Networks. IEEE Access, 8, 178825-178834, 2020.
[20] Ding, L., Wang, Z., Wang, X., & Wu, D. Security information transmission algorithms for IoT based on cloud computing. Computer Communications, 155, 32-39.
[21] Ganapathy, S. A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Computer Networks, 151, 181-190.
[22] Ouda, G. K., & Yas, Q. M Design of cloud computing for educational centers using private cloud computing: a case study In Journal of Physics: Conference Series (Vol. 1804, No. 1, p. 012119).
[23] Qin, Q. , Jin, B. , & Liu, Y., A secure storage and sharing scheme of stroke electronic medical records based on consortium blockchain, BioMed Research International, 2021(5), 1-14, 2021.

Edited by: Pradeep Kumar Singh
Special issue on: Intelligent Cloud Technologies Enabled Solutions for Next Generation Smart Cities
Received: Nov 14, 2022
Accepted: Nov 1, 2023