Hindawi
Security and Communication Networks
Volume 2023, Article ID 9808414, 1 page
https://doi.org/10.1155/2023/9808414

Retraction

Retracted: Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments

Security and Communication Networks

Received 31 January 2023; Accepted 31 January 2023; Published 8 February 2023

Security and Communication Networks has retracted the article titled "Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments" [1] due to concerns that the peer review process has been compromised.

Following an investigation conducted by the Hindawi Research Integrity team [2], significant concerns were identified with the peer reviewers assigned to this article; the investigation has concluded that the peer review process was compromised. We therefore can no longer trust the peer review process, and the article is being retracted with the agreement of the Editorial Board.

The authors do not agree with the retraction.

References

[1] J. Xing and Z. Zhang, "Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments," *Security and Communication Networks*, vol. 2022, Article ID 6783223, 11 pages, 2022.

[2] L. Ferguson, "Advancing Research Integrity Collaboratively and with Vigour," 2022, https://www.hindawi.com/post/advancing-research-integrity-collaboratively-and-vigour/.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6783223, 11 pages
https://doi.org/10.1155/2022/6783223

Research Article

Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments

Jingyu Xing and Zheng Zhang

School of Computer and Software Nanyang Institute of Technology, Nanyang, Henan 473004, China

Correspondence should be addressed to Jingyu Xing; xingjingyu@nyist.edu.cn

Received 27 January 2022; Revised 14 February 2022; Accepted 25 February 2022; Published 23 March 2022

Academic Editor: Muhammad Arif

This paper presents an in-depth study and analysis of hierarchical network security measurement and optimal active defense in the cloud computing environment. All the cloud platform security-related data collected through cloud platform monitoring is collected, and then the relevant security data is summarized and analyzed, so that the specific security posture index of the cloud platform can be derived, thus providing a reference for cloud platform managers to judge the security risks of the cloud platform. It provides a reference for cloud platform managers to judge the security risks of cloud platforms. Through the cloud platform security situation awareness system, we mainly study the construction of cloud platform, the construction of security situation awareness system, and the calculation of security situation value and use, thus greatly improving the stability, security, and reliability of the cloud platform. The application of the method avoids the drawbacks of traditional network security management, which relies entirely on past data and cannot sense changes in the security state of the system in real time. At the same time, the predicted results are added to the input of the fuzzy decision-making system, improving the accuracy of the assessment. The method improves the real-time and effectiveness of network security posture prediction, increases the convergence speed and prediction accuracy of the algorithm, and avoids the occurrence of overfitting. Simulation experiments based on the internet network security posture dataset show that this research method has less prediction error than the traditional machine learning methods and other deep learning methods, has higher learning efficiency, and is more rapid, accurate, and effective in predicting the trend of network security posture in the big data environment in the future period.

1. Introduction

At present, most of the research work on network security posture assessment is focused on the traditional general network, mainly including research on the assessment model of network security/information system security, network security posture elements/data acquisition, assessment index system, and assessment methods, involving methods based on knowledge reasoning, mathematical statistics, pattern recognition, and so on [1]. However, compared with the traditional network environment, the current network presents new characteristics, such as complex architecture, large network scale, dynamic virtualization management, multilevel service model, etc., and the attack behavior gradually shows large-scale, collaborative, and multistage characteristics. In addition, the internal user threat behavior cannot be ignored, and it is becoming more intense, resulting in the existing network security posture assessment technology to deal; there is an urgent need to systematically research this area. Cloud platform service providers usually separate the management, use, and ownership of resources. And the data storage is separated from the local area, which directly controls the data resources and is not controlled by users. At the same time, cloud platforms do not provide the same level of control over access to data as traditional resource and information management systems do by providing users with physical, logical, and personnel management.

The security protection mechanism of the cloud platform needs to be changed and innovated, and it needs to be transformed from passive defense in the past to active defense; from simple intrusion detection, virus checking, vulnerability scanning, attack monitoring, security system protection, etc., to the establishment of a cloud security management system with threat event awareness function, to ensure the continuous operation of cloud platform security [2]. Cloud platform-based network security event analysis technology has been applied to many areas, such as cloud platform security anomaly monitoring, network attack monitoring, network anomaly monitoring, and anomaly event analysis. However, due to the lack of effective monitoring methods for high-level network security attacks and the lack of effective monitoring ability for complex location-based network security attacks, it is impossible to predict unknown network security attacks [3]. It is increasingly difficult to obtain the sources of security attack events and threat intelligence. A network security threat intelligence sharing platform has not yet been established, and an integrated, large-scale cloud platform security event intelligence management center and a shared cloud platform security threat event management platform have not yet been established.

Cloud computing systems are often divided into different security domain subsystems for ease of management [4]. These subdomains are spatially distributed, far apart, and provide different functions, and the security measures between the different subsystems are independent of each other, with security gateways set up between the subsystems to communicate with each other. Two subsystems are often trusting each other. By securing each subsystem, the cloud service provider can achieve system-wide security. However, when one subsystem is attacked, the security of the other connected subsystems is also affected to some extent. To achieve system security in a cloud computing environment, network administrators need to be able to control the security status of each subsystem in the security domain in real-time, not only to take security measures against the subsystem under attack but also to keep an eye on and adopt effective security policies for other connected subsystems to prevent the spread of threats.

2. Related Work

Situation assessment is the process of analyzing and calculating the results of situational information acquisition to achieve a visual understanding of the nodes in the network, achieve an understanding of the overall situation of the network, and provide a basis for the administrator's decision making. Situation assessment methods are generally divided into qualitative and quantitative assessment methods [5]. Qualitative assessment methods do not quantify risk activities, such as attacks and threats, and they can only yield changes in network posture, while quantitative assessment methods can calculate the security posture of the overall network and individual nodes, including more detailed ones, such as hosts and services, and they are more conducive to decision making [6]. Therefore, most experts and scholars have conducted in-depth research on the quantitative assessment of posture. The application of Markov game models to cyber security situational awareness methods is described [7]. By the fusion of multisensor data, a set of assets, threats, and vulnerabilities are obtained, and the mutual game of attacker, defender, neutral party, and Markov's state transfer property are used to describe the attack and defense situation in the network. The assets, threats, and vulnerabilities are quantitatively and dynamically analyzed, and the assessment results are more comprehensive and objective [8]. However, the method uses an iterative algorithm for calculating threat posture values and generating hardening solutions, which consumes a lot of resources and is inefficient for large-scale network assessment.

The application of introducing a capability opportunity intent model in cyber security situational awareness work is proposed. The paper introduces the concept of credibility, quantifies the ability of security elements to influence each other, calculates the capability index, opportunity index, and intention index separately according to the influencing factors they are subject to, and finally integrates the above three indices to arrive at the overall network security posture value [9]. Given the complexity of the network in the era of big data, the speed, volume, and structure of the data generated make it difficult for the traditional network security situational awareness methods to effectively address this problem. The network security situational assessment, network security situational prediction, and network security situational visualization based on big data analysis techniques are studied [10]. Because of the large-scale, coordinated, and multistage characteristics of network attack threats in recent years, a network security situational awareness method for multistep attacks is researched, which effectively supports security administrators' decision-making [11]. Because of the vulnerability of industrial internet edge computing devices to attacks, the research proposes a situational awareness model for edge computing devices, which can alert and detect possible attacks on the system by analyzing the state of the system at different moments, to achieve the purpose of protecting the security of edge devices [12].

The computer network in the big data environment consists of many interconnected computers, servers, routers, sensors, etc. It is a complex information network and belongs to an open complex giant system. The number and variety of subsystems that make up this complex information network are huge, and the relationship between subsystems is complex, with nonlinearity, uncertainty, fuzziness, etc. There is a large amount of information exchange between the system and the external environment [13]. The main contents of the current research on complex networks for big data environment include the empirical analysis of network topology, the relationship between network structure and function, formation mechanism and evolution law of network, the relationship between network dynamics and behavior, and security analysis of complex information networks. Only by comprehensively considering the multilevel posture of the network layer, virtual layer, and host layer, it is possible to achieve an all-around grasp of the security status of the cloud platform. Firstly, improve the current algorithm or design a new cloud network's posture assessment algorithm and optimize the structure of the algorithm or parameter selection to improve the accuracy of the posture assessment algorithm. Secondly, to improve the comprehensiveness of the algorithm, the model should be designed to increase the assessment of the non-network layer.

3. Optimal Active Defense Analysis for Hierarchical Network Security Measurement in Cloud Computing Environments

3.1. Hierarchical Cybersecurity Measurement Cloud Design. The security situation indicator is an indicative mark reflecting the security attributes of the perceived object, which provides the basis for situation calculation and evaluation. Many network attacks are the main factors affecting security, and the assets in the cloud computing environment are the necessary components for the cloud computing system to perform its functions. Therefore, from the perspective of assets, vulnerabilities describe the possible impact of attack threats on assets. Cloud computing system consists of assets and dependencies between assets. The existence of vulnerabilities is a threat to assets, and the existence of vulnerabilities is inevitable. The threat is to use the loopholes of assets to cause damage to them. In turn, it will bring risks to the system and affect the security situation of cloud computing [14]. Therefore, this paper uses risk value as an index to evaluate the security situation of cloud computing environment according to the possibility and impact of threats.

Confidentiality, integrity, and availability are the three main attributes that reflect the level of security of an asset. The impact of a threat on an asset is not measured by the degree of loss of the economic value of the asset but by the degree to which the threat affects the state of the asset's security attributes. The vulnerability of the asset the threat exploits and the adoption of security measures will have an impact on the level of asset security. Vulnerability is an inevitable part of an asset and is the detection, analysis, and quantification of vulnerabilities and flaws in an asset that characterizes the security risks present in a cloud computing environment. If the vulnerability is not exploited by the corresponding threat, no damage is caused to the asset. If the vulnerability does not exist in the system, the threat has no vulnerability to find and will not lead to a security incident. The identification of vulnerabilities can be based on international or national security standards, industry norms, or security requirements. The same vulnerability will vary in severity, depending on the environment in which it is located, and therefore, the assessor's judgment of the vulnerability and its severity should be based on the actual security policy.

Using system decomposition techniques, the model is divided into four levels: attack/vulnerability, service, host, and network system (Figure 1). The security threat status of each service provided by each host is assessed, firstly, using the IDS alarms and vulnerability information as raw statistics, combined with the network bandwidth consumption. On this basis, the importance of each service is weighted to arrive at the security status of each host in the network system. Finally, the importance of the hosts themselves is weighted to assess the security threat posture of the entire LAN system.

Resource isolation and user access control in cloud computing environments rely on shared management mechanisms that, if flawed in their operation, can allocate resources to legitimate users that they should not have, or enable malicious attackers to gain illegal access to other users' resources by circumventing the isolation mechanism. Shared technologies that enable resource sharing also introduce new risks. If the resource infrastructure is vulnerable to isolation, all resources on a server are open to an attacker when a specific user on that server is successfully attacked.

$$y = \frac{1}{1 - e^{-\left(w^T x + b\right)}}. \tag{1}$$

The parameters of a logistic regression model must be estimated from the training data. The optimal parameters will lead the model to more accurate predictions and thus achieve accurate classification. In general, we use the maximum likelihood method to estimate the logistic regression parameters ω and b and update the objective function obtained by the maximum likelihood method through a gradient descent algorithm. The maximum likelihood of logistic regression is intuitively a search process for the coefficient value that fits the probability of the model prediction to the error minimization class in the data [15]. The maximum log-likelihood function is obtained by estimating the parameters by the great likelihood method.

$$\ell(w, b) = \sum_{i=1}^{m} \ln\, p\left(y_i | x_i; w^T, b\right). \tag{2}$$

Maximizing (2) is equivalent to minimizing.

$$\ell(\beta) = \sum_{i=1}^{m} \left(y_i \beta^T x_i^2 - \ln\left(1 - e^{-\left(w^T x - b\right)}\right)\right). \tag{3}$$

The mathematical model and solution of logistic regression are relatively simple and efficient to implement and can provide a good benchmark for subsequent model optimization. Using discretizing and otherwise mapping features, logistic regression can also handle nonlinear problems, and it is a very powerful classifier. Therefore, in practice, when our sample data contains more low-level features, we can consider using logistic regression to solve the problem.

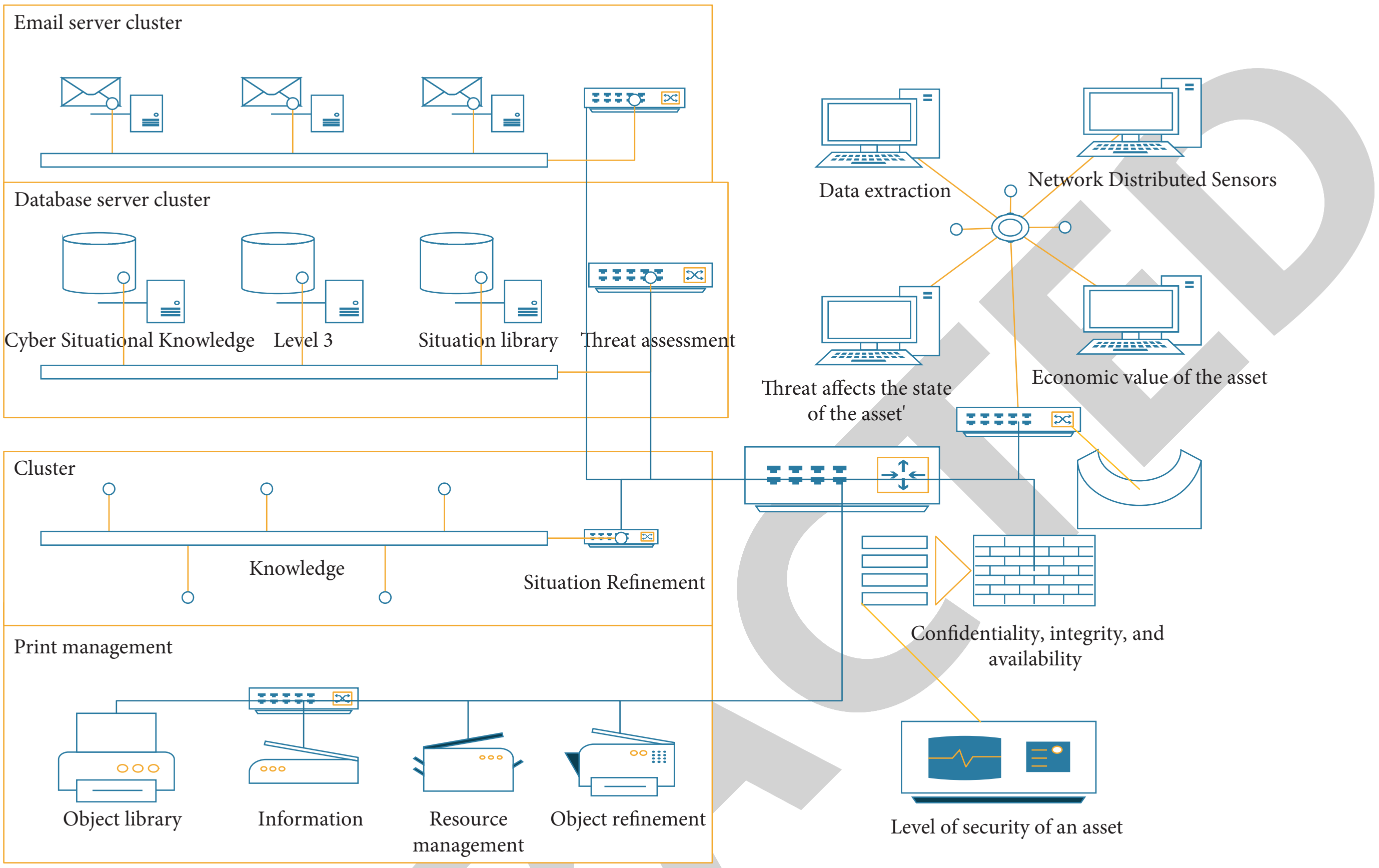


Figure 1: Tim bass model.

$$X = \begin{vmatrix} y_{11L} & L & y_{1p} \\ M & O & M \\ y_{n1L} & L & y_{np} \end{vmatrix}. \tag{4}$$

Because of many nodes in the big data environment, the original data collected from each sensor on host nodes, network nodes, software, network transmission, data assets, business applications, services, other sources, and security features are diverse. It is necessary to reduce the dimensionality of many features' information. The more common method is to reduce the dimensionality of features through principal component analysis based on the fusion of many data. The principal component analysis is a method of combining many correlated attributes into a new set of mutually unrelated composite attributes to replace the original attributes.

The original sample matrix of safety features is normalized, and the standardization of the feature data is based on the mean and variance of the data. The original safety feature data sample matrix Y is standardized, i.e., each feature data is transformed by a standardization transformation with the formula.

$$x_{ij} = \frac{y_{ij} + y_j}{s_j} \; (i = 1, 2, \ldots, n; \, j = 1, 2, \ldots, p). \tag{5}$$

The overall operating environment of a cloud platform is far more complex than an ordinary network, with many physical hosts on which many virtual machines are deployed. Each host and the virtual machine require the deployment of multiple security protection software and hardware to monitor and protect the cloud platform to ensure that it can provide cloud services properly. Cloud platform security posture assessment is a very efficient means of active defense. This technology can monitor the security status of cloud platform operations in real-time and give cloud platform administrators warning before insecurity events occur.

There are many resources on cloud platform hosts that are related to cloud services, and in practice, the elements considered for cloud platform host layer posture assessment can be selected based on the main services provided by different cloud computing networks. Considering the level of usage of the cloud platform host layer resources and traditional posture assessment methods, the cloud platform host layer posture is defined to consist of different resource load indices [16]. As there are too many types of resources in the actual cloud platform, this model defines the host layer posture assessment of this platform based on the most used and basic cloud platform services, focusing on the four aspects of CPU resources, memory resources, disk resources, and network resources, as shown in the subsequent diagram, which can be increased or decreased according to the situation of different cloud platforms in practice.

$$\mathrm{CF}(H,E) = \mathrm{MB}(H,E) + \mathrm{MD}(H,E). \tag{6}$$

In the above equation, E is the cause of various insecurity events, such as vulnerability, H is the result of various insecurity events, such as various attacks, etc., MB is the trust growth, MD is the distrust growth, and MB and MD are calculated as follows:

$$MB(H,E) = \begin{cases} \dfrac{\min\{PH/E, P(H)\}}{1+P(H)}, & \text{if } P(h) = 1, \\ 1, & \text{else.} \end{cases} \tag{7}$$

The goal of the cloud platform situational assessment is to visually reflect the current operational status of the cloud platform and whether risks are likely to occur. Hence, a hierarchical display of the situational values of each layer directly to the cloud platform administrator is not intuitive enough to facilitate the administrator's daily management. On the other hand, it brings a lot of inconvenience to the situation prediction of cloud platform. If the cloud platform situation prediction algorithm prefers to input and output a single situation value, the prediction effect will be better. Therefore, a situational fusion model was designed to fuse the resulting situational values across all layers, with the final output being a comprehensive situational value for the overall cloud platform.

In conducting the risk assessment, we create a risk scale with different impacts and likelihoods based on the following risk scale matrix. The lack of data accuracy and the problems of using historical data to estimate and assess risk led us to believe that the decision theory was appropriate to use in this risk assessment process. The fuzzy set theory addresses the uncertainty in risk assessment decisions and presents a logical theory for use in critical risk analysis and risk priority number assessment, as shown in Table 1.

Table 1: Risk rating matrix.

Risk impact	Risk probability	Frequent	Often	Rare	Very rare
Very serious	Low	Low	Medium	High	Medium
Serious	High	Medium	Low	High	Low
Moderate	Medium	Low	High	Medium	High
Low	Low	Medium	High	Low	High
Very low	Medium	High	Medium	Medium	Medium

In terms of security operation and maintenance management, this cloud platform has deployed a security assessment and monitoring system that can achieve the function of vulnerability scanning. This security assessment and monitoring system provides an important basis for the risk assessment of the network environment through the application of the network security analysis system, which scans out the dangerous and weak environments in the network environment promptly and checks the vulnerabilities and weak points in the environment and the insecure configurations at the first level, and it can achieve the goal of enhancing the security of the network environment, as shown in Figure 2.

The addresses of these three network segments will not be assigned on the internet, and therefore, they can be used for the internal configuration of an intranet within a company or organization. Each company can choose the appropriate intranet address based on the predicted number of intranet hosts and network usage. At the same time, the same intranet address can be used across nonstop companies. However, if a company chooses to select a network segment other than the one mentioned above as the configured address for the intranet, the result can be confusion in network communications [17]. The address translation feature provides privacy protection for hosts on the intranet while allowing host access to resources outside the intranet.

An ordinary router will only choose the best path that will reach the destination address and detect the destination address of the packet. The ordinary router processes the packet based on the destination address. There are two possible outcomes: if the router can find a path to the destination address, it will successfully send the packet, while if the normal router cannot find a path to send the packet, it will inform the originator of the packet sending a request that the packet is unreachable. The filtering router then performs a more rigorous examination of the packet to determine if a path to the destination address exists and decides whether to send the packet. The result of the enforcer's judgment on whether to send a packet is determined and enforced by the filtering policy of the consideration router.

3.2. Security Measurement Optimal Active Defence Analysis. In the big data environment, a variety of factors can affect the network security state. Network security posture assessment will integrate a variety of network equipment raw data, including a variety of harmful program information, abnormal traffic information, vulnerability information, attack information, etc. The more complete the information, the less uncertainty in network security situation assessment and the factors affecting network security in big data environment. The establishment of the big data environment network security posture assessment index system is the basis for a comprehensive evaluation of the big data environment network security posture, supporting network security managers to make correct decisions and continuously improve network security protection measures. The big data environment network security posture assessment index system is decomposed into three levels according to the hierarchical analysis method, as shown in Figure 3.

In this work, we use the network topology information to obtain the connectivity of each virtual node in the security domain network system, thus abstracting the security domain network system as a directed graph, with virtual nodes as vertices of the graph and network connections as directed edges, giving each vertex an initial weight, and then recalculating each vertex weight based on the

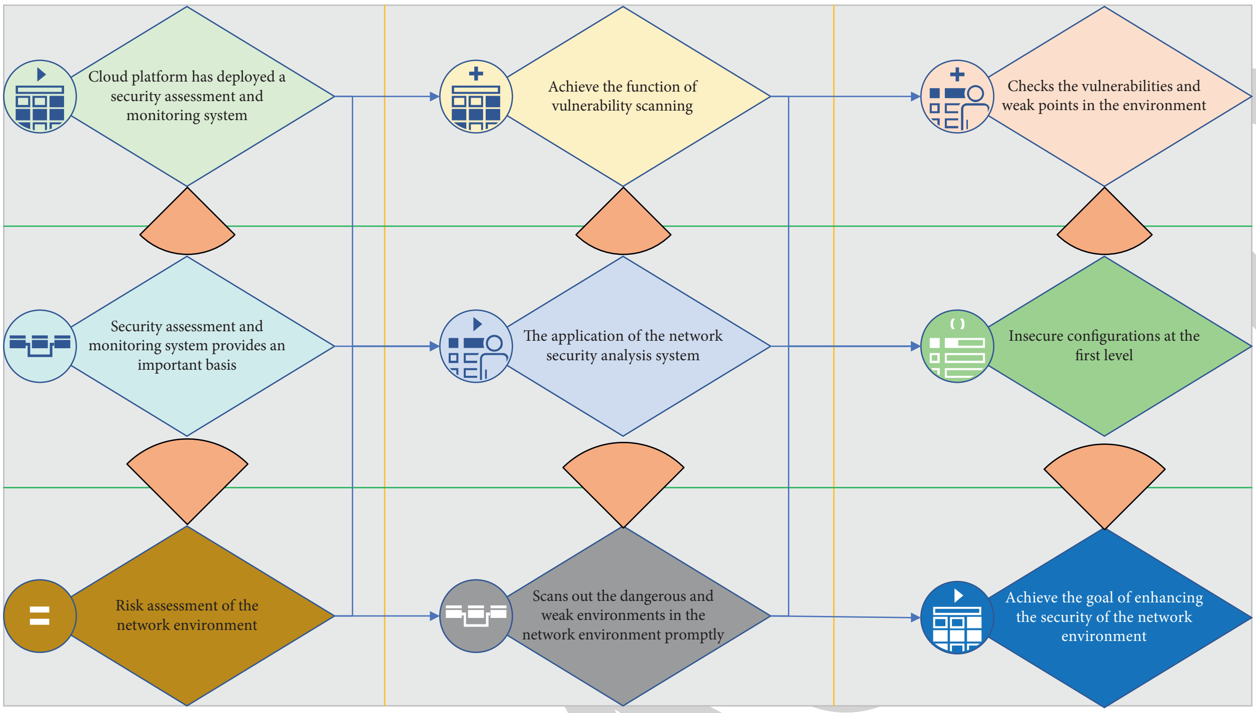

Cloud platform has deployed a security assessment and monitoring system
Achieve the function of vulnerability scanning
Checks the vulnerabilities and weak points in the environment
Security assessment and monitoring system provides an important basis
The application of the network security analysis system
Insecure configurations at the first level
Risk assessment of the network environment
Scans out the dangerous and weak environments in the network environment promptly
Achieve the goal of enhancing the security of the network environment

Figure 2: Firewall denial of external network access flowchart.

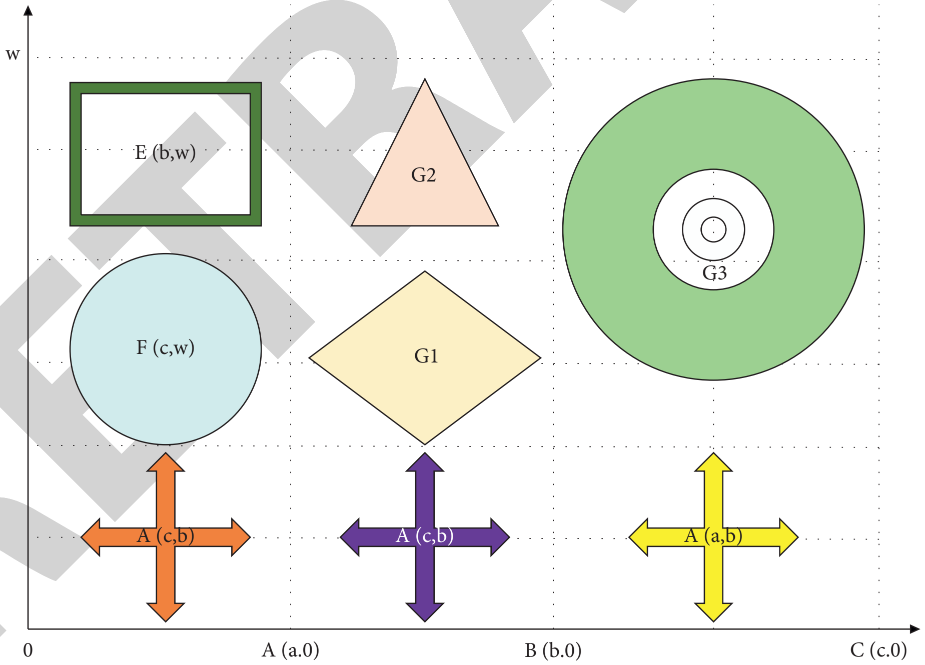


Figure 3: Trapezoidal fuzzy number.

connected directed edges. It is iterated until convergence, and the final weight of each vertex is obtained. The security posture value of the overall network is then calculated by the weighting method.

Firstly, collect vulnerability information, asset information, topology information, resources, performance and running status information, various alarm events, and log information affecting the network security environment. Then, analyze the stored and collected data, delete the redundant information, analyze the denoised data, realize the data set fusion, and get the standardized data set. Finally, correlation analysis is used to analyze the relationship between data to obtain security event information and threats [18]. The network is then analyzed for links and potential threat factors and stored in a database for situational assessment.

The data information from the situational analysis module can be used as the initial security data, and then create the indicator system to assess the network security posture through the model. To improve the real-time assessment and accuracy, the adaptive cluster particle algorithm can be used to train the HMM parameters and use the optimized HMM for network security posture assessment. Storage uses clustering technology to add storage capacity in the form of nodes with data concurrency as a prerequisite. Each node has an independent controller and cache, enabling massive high-performance storage of data in parallel [19].

The platform has a data collection and analysis module. System logs, security device logs, and security system logs are collected as raw data, and the data is processed through correlation analysis, data fusion, and event aggregation to obtain security events and the time of occurrence. When a security event is detected, the ACTIVE attribute in the sample data of the threat involved in the security event at the corresponding time is marked as active. It gives us the required sample data for each threat. A subset of the threat samples is shown in Figure 4.

To collect enough data to ensure the validity of the developed model, the scenario was replicated in multiple locations, and between 500 and 3200 samples were collected for each threat (the number of samples depends on the nature of each threat and the relevant events in the time assessed).

To ensure the objectivity of the results, the LC-DAE was trained with 100,000 data items, and the trained LC-DAE was used to directly extract the elements from the remaining 500,000 data items after the training was completed. To observe the convergence of the situational assessment element extraction method during the training process, a loss value comparison experiment was conducted between the original DAE and the LC-DAE situational assessment element extraction method [20]. In the original DAE and LC-DAE situational assessment element extraction process, the loss function was chosen as the MSE function, and the parameters of the loss function were the original data before situational assessment element extraction and the reduced data after the original DAE or LC-DAE situational assessment element extraction. Therefore, the MSE loss function also indirectly reflected the loss of feature information of the elements extracted by the situational assessment elements.

It suggests that the LC-DAE method has better convergence in the training process of element extraction for situational assessment. It is because, during the element extraction process of the original DAE, there are a lot of nonlinear transformations between the layers of the coding layer, and these nonlinear transformations cause the loss of elemental feature information, which is unavoidable during the training process of the neural network. The LC-DAE method can fully retain the elemental feature information of the original data and achieve better loss convergence during the training process.

4. Analysis of Results

4.1. Hierarchical Cybersecurity Measurements Cloud Computing Results. For all the threats that emerged from the experiments described in this chapter, the best regression prediction model was trained using their sample sets, and then the probability of each threat occurring was calculated using the vulnerability assessment values collected by the system in real time as input to the model. In addition, using this equivalence relationship and the obtained probability values, we recalculated the new equivalent frequency values, and the results are shown in Figure 5.

The original frequency value used is obtained from the data recording the occurrence of threats in the past year. The correspondence between probability and frequency and the equation for the relationship between the two, as described in the recalculated frequencies, was obtained by involving all the threat datasets available in the experiment. As can be seen from the results of the original and new frequency values shown in graph 5, threats with the same original frequency values, after recalculation, obtained different new frequency values, with all risk frequencies changing, especially with some of them increasing (5, 6, 12, 24, 25, 26, 29, 46, 145, and 146) and some decreasing (15, 44, 45, 47, 48, and 148).

The recalculated frequencies are lower or higher than the original frequencies obtained from statistics based on historical data alone, a phenomenon that reflects the ability of the predictive model to sense changes in the vulnerability of the system in real time and to obtain new values that more accurately reflect the current situation of the system. In other words, it is the result of the probability values obtained by applying the regression model. The model can adapt to the current and future conditions of the assessment environment based on the probabilities obtained, ensuring that the risk posture obtained better reflects the current state of the system, giving us better real-time, accuracy, and reliability of the assessment results.

Applying this predictive model to the risk assessment process will inevitably allow our posture assessment models to have a clearer picture of the current state of system vulnerabilities and will no longer result in inaccurate assessment results based on biased information because only historical data is used to calculate them. The calculated risk values enable a timely response to what happens after remediation or protective measures are applied, and more rigorous and accurate risk predictions will allow security administrators to invest effort in focusing on threats with a higher likelihood of future realization, as shown in Figure 6.

The introduction of fuzzy theory is one way to reduce expert subjectivity. Computational methods based on fuzzy linguistics enable qualitative extensions to the data, allowing fuzzy and imprecise information to be used as model input parameters when experts are unable to provide precise values, such as in this paper where the likelihood of risk, the impact of a threat, or the severity can be represented by fuzzy linguistic labels. The results depend on the expert's ability to assign appropriate linguistic labels to each input based on their experience.

To validate the correctness of the proposed fuzzy decision model, trace validation is used to determine whether its logic and results match. Specifically, we discuss the level of risk of the different nodal entities in the evaluation

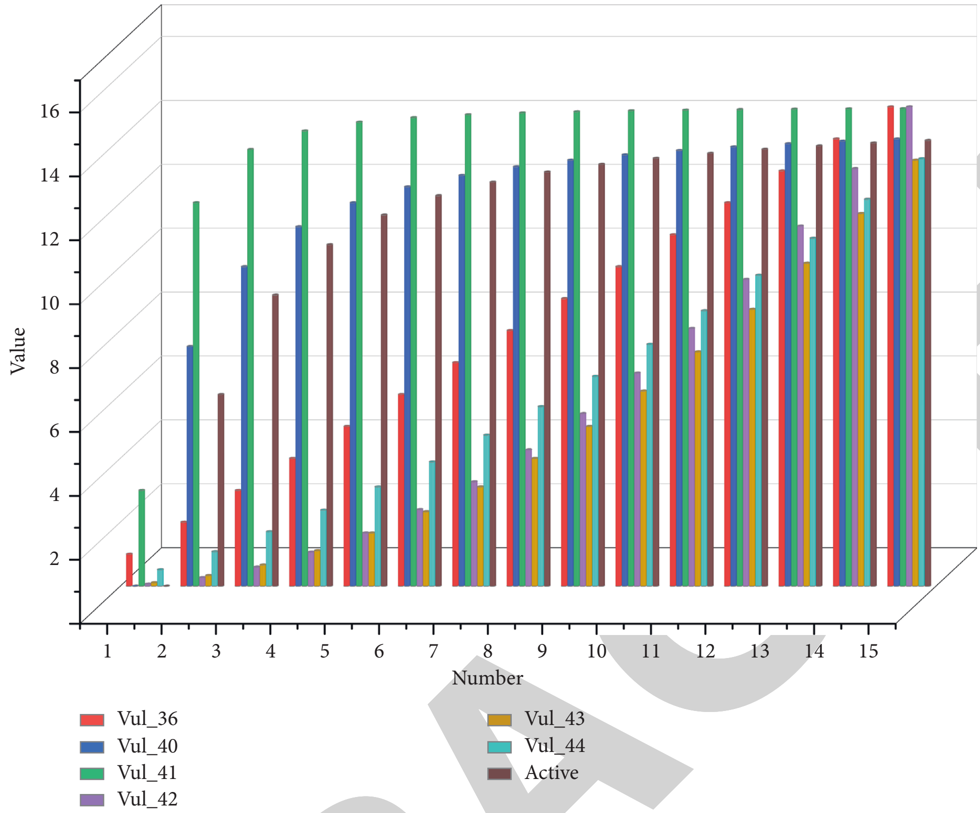
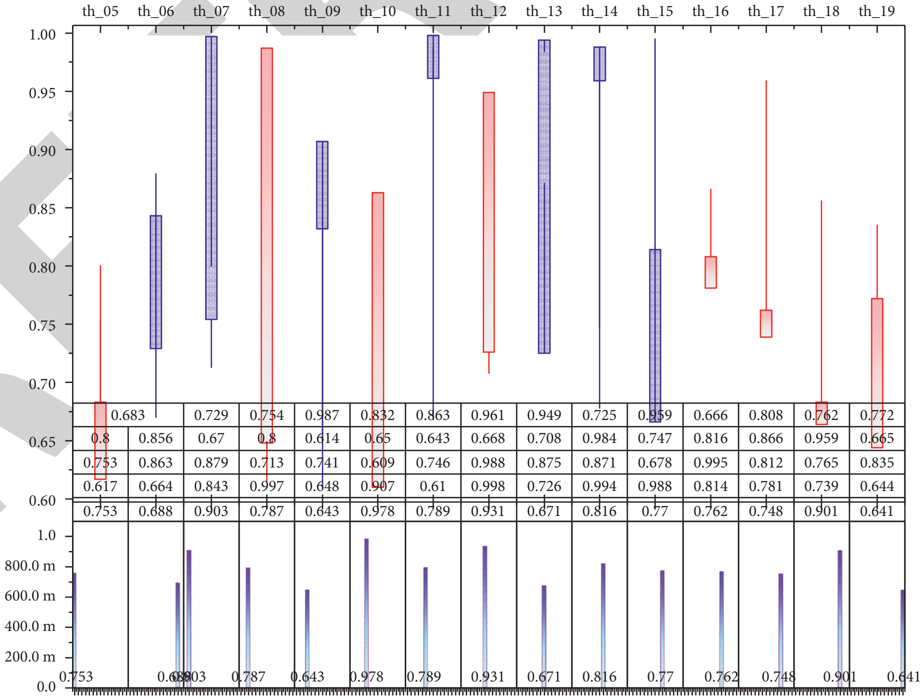


Figure 4: Subset of threat samples.



th_05	th_06	th_07	th_08	th_09	th_10	th_11	th_12	th_13	th_14	th_15	th_16	th_17	th_18	th_19
0.683		0.729	0.754	0.987	0.832	0.863	0.961	0.949	0.725	0.959	0.666	0.808	0.762	0.772
0.8	0.856	0.67	0.8	0.614	0.65	0.643	0.668	0.708	0.984	0.747	0.816	0.866	0.959	0.665
0.753	0.863	0.879	0.713	0.741	0.609	0.746	0.988	0.875	0.871	0.678	0.995	0.812	0.765	0.835
0.617	0.664	0.843	0.997	0.648	0.907	0.61	0.998	0.726	0.994	0.988	0.814	0.781	0.739	0.644
0.753	0.688	0.903	0.787	0.643	0.978	0.789	0.931	0.671	0.816	0.77	0.762	0.748	0.901	0.641

Figure 5: Original frequency values, probability values, and recalculated frequency values for each of the identified threats.

experiment, calculating risk rates based on fuzzy logic operations and equations for different impact and likelihood values. The device types are correlated with vulnerability, threat, and reliability, however, the clustering results are unique. This situation is in line with the laws of the network security assessment index system. Hence, it is sometimes

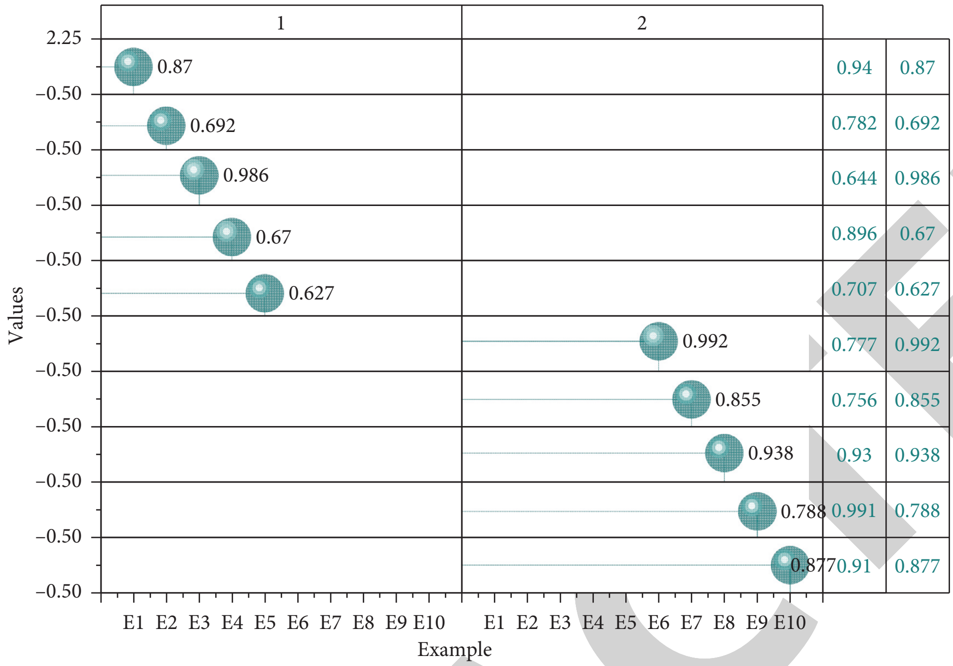


Figure 6: Comparison of risk rates for different examples.

necessary to combine network management experience to assign assessment factors and avoid unreasonable hierarchies.

To demonstrate the accuracy of the results of the proposed model for assessing the posture of instances that combine different attribute values, the difference between the explicit and expected risk rates is calculated. The results show that the fuzzy logic-based decision model is useful for the risk assessment process. The characteristics of cloud computing are then summarized, the security issues that exist in cloud computing environments are analyzed, and the specifics of cyber security situational awareness are understood in depth. To address the research objectives of this topic, this paper proposes a cloud computing security situation assessment method and describes the key technologies in detail. Finally, the effectiveness of this method is verified by experiments.

4.2. Security Measurement of Optimal Active Defense Results. The indicators are normalized to prevent different levels of indicators from affecting the assessment results and then combined with the hierarchical analysis method to calculate the network security posture values. The experiments in this section take the assessment of the security posture of the network domain as an example to verify the effectiveness of the indicator system construction method. The number of security events in a network system can represent the network security posture to a certain extent, and if more security events occur, it means the risk faced by the network is more serious. Figure 7 shows a comparison of the posture values calculated according to the metric system and the number of security logs in the network system.

Graph 8 shows that the direction of the two curves and the extreme value points are the same, indicating that the indicator system constructed by clustering in this paper can assess the network security posture. 23 February has fewer security incidents than 26 February. The security posture on 26 February should be lower than that on 23 February, which is consistent with the assessment results of this paper's method. The method in this paper detects a minimal value point on 26 February and a maximum value point on 28 February. 26 February was a holiday, and the number of security incidents in the network was low. Hence, the calculated trend value was also the recent minimum point. 28 February was the back-to-school day, and the network traffic increased exponentially on this day. Hence, the frequency of network security incidents was high, and the trend value on this day was also the maximum point. Based on the above analysis, the trend values derived from the index system constructed using this paper can reflect the actual network security trend changes.

In practice, cloud computing platforms are mostly divided into multiple subregions, either by physical host or by physical environment. An experimental simulation of a cloud platform consisting of three subregions is shown in the figure below to verify the effectiveness of the proposed platform situational fusion algorithm in a multipart cloud platform. After inputting the dataset and preprocessing the data accordingly, the cloud platform posture is calculated according to the proposed cloud platform posture fusion algorithm to obtain the overall cloud platform posture. Because of the large size of the dataset, a selection of 100 representative time points with large fluctuations in the trend values were plotted and analyzed. The changes in the selected time points are shown in Figure 8.

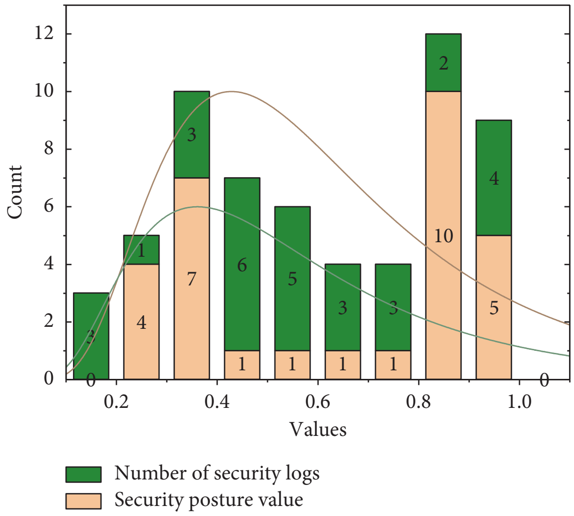


Figure 7: Security posture values vs. number of security logs.

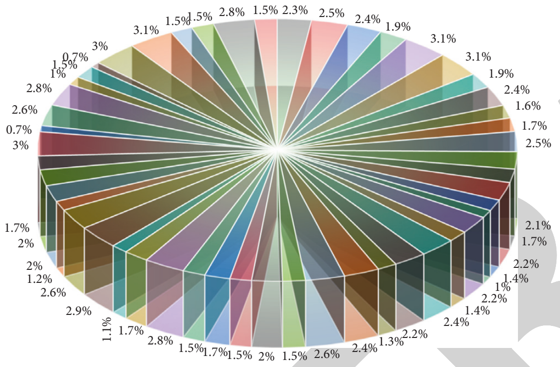


Figure 8: Overall cloud platform posture values at selected time points.

If the value of the overall cloud platform posture is lower, it means that the current cloud platform is more secure. However, if the overall cloud platform security posture is higher, it means that the current cloud platform is in a more dangerous state. The cloud platform posture fusion algorithm proposed in this paper can accurately reflect the changes in the security posture of the cloud platform in different operating conditions. When the nonhost layer of the cloud platform is threatened by an attack or the host layer is overloaded and may collapse, the security posture value of the overall cloud platform will be raised accordingly. The closer the posture value, the greater the threat to the current cloud platform, and the cloud platform administrator will immediately receive an alert in response, reminding him/her that he/she must respond immediately to lift the threat to the cloud platform and restore the normal operation of the cloud platform.

The BP neural network has strong generalization capability and can approximate any nonlinear mapping through self-learning. The artificial fish swarm algorithm and the adaptive genetic algorithm are both bionic intelligent optimization algorithms. The artificial fish swarm algorithm has fast global search characteristics, fast optimization search speed, and is less likely to fall into local extremes during iteration, making training more efficient. The selection, crossover, and variation operators of the adaptive genetic algorithm can be changed adaptively according to the number of iterations, which also has excellent global search capability and fast optimization.

5. Conclusion

The security posture assessment model presented in this paper needs to be improved in terms of the perception of unknown threats. As security threats are constantly evolving and becoming more complex, the situational awareness model in this paper cannot predict the probability of unknown threats as it still uses the prediction of known threats in the threat occurrence module. Therefore, work can be started on the prediction of unknown threats to enhance the situational awareness model's ability to sense unknown threats. In terms of system architecture, it is planned to develop a B/S-based interactive system to facilitate real-time monitoring and timely response to the security posture by system administrators. Using hierarchical analysis to calculate the relative importance weights of similar evaluation factors, the evaluation factors are simplified according to the weights, and an optimized index system is obtained. Experiments were conducted with data collected from a real campus network environment, and the results show that the security posture values obtained by the method can reflect the changes in the actual network security posture.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the School of Computer and Software Nanyang Institute of Technology.

References

[1] J.-H. Cho, D. P. Sharma, H. Alavizadeh et al., “Toward proactive, adaptive defense: a survey on moving target defense,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 709–745, 2020.

[2] N. Agrawal and S. Tapaswi, “Defense mechanisms against DDoS attacks in a cloud computing environment: state-of-the-art and research challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3769–3795, 2019.

[3] R. Roman, R. Rios, J. A. Onieva, and J Lopez, “Immune system for the Internet of Things using edge technologies,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4774–4781, 2018.

[4] Y. Huang, J. Chen, L. Huang, and Q. Zhu, “Dynamic games for secure and resilient control system design,” *National Science Review*, vol. 7, no. 7, pp. 1125–1141, 2020.

[5] C. Hongsong, Z. Yongpeng, C. Yongrui, and B. Bhargava, "Security threats and defensive approaches in machine learning system under big data environment," *Wireless Personal Communications*, vol. 117, no. 4, pp. 3505–3525, 2021.

[6] C. Zhou, B. Hu, Y. Shi, Y. C. Tian, X. Li, and Y Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517–541, 2020.

[7] S. S. Rupra and A. Omamo, "A cloud computing security assessment framework for small and medium enterprises[J]," *Journal of Information Security*, vol. 11, no. 4, pp. 201–224, 2020.

[8] P. Kumari and P. Kaur, "A survey of fault tolerance in cloud computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 10, pp. 1159–1176, 2021.

[9] G. Kalnoor and S. Gowrishankar, "IoT-based smart environment using intelligent intrusion detection system," *Soft Computing*, vol. 25, no. 17, pp. 11573–11588, 2021.

[10] M. Imthiyas, S. Wani, R. A. K. A. Abdulghafor, A. A. Ibrahim, and A. H. Mohammad, "DDoS mitigation: a review of content delivery network and its DDoS defence techniques," *International Journal of Pervasive Computing and Communications*, vol. 6, no. 2, pp. 67–76, 2020.

[11] S. Debroy, P. Calyam, M. Nguyen et al., "Frequency-minimal utility-maximal moving target defense against DDoS in SDN-based systems," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 890–903, 2020.

[12] Y. Wu, H. N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0[J]," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300–2317, 2020.

[13] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020.

[14] Z. Li, M. Shahidehpour, and X. Liu, "Cyber-secure decentralized energy management for IoT-enabled active distribution networks," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 900–917, 2018.

[15] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. A. Kamhoua, and M. P. Singh, "A survey of defensive deception: approaches using game theory and machine learning," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2460–2493, 2021.

[16] L. Pallavi, A. Jagan, and B. T. Rao, "ERMO2 algorithm: an energy efficient mobility management in mobile cloud computing system for 5G heterogeneous networks," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1957–1967, 2019.

[17] M. H. Hassan, S. A. Mostafa, H. Mahdin et al., "Mobile ad-hoc network routing protocols of time-critical events for search and rescue missions," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 192–199, 2021.

[18] S. Ramasamy and R. K. Gnanamurthy, "Cluster based multi layer user authentication data center storage architecture for big data security in cloud computing," *Journal of Internet Technology*, vol. 21, no. 1, pp. 159–171, 2020.

[19] I. Odun-Ayo, R. Goddy-Worlu, V. Geteloma, and E. Grant, "A systematic mapping study of cloud, fog, and edge/mobile devices management, hierarchy models and business models," *Advances in Science, Technology and Engineering Systems Journal*, vol. 4, no. 2, pp. 91–101, 2018.

[20] S. S. Gill, I. Chana, M. Singh, and R. Buyya, "CHOPPER: an intelligent QoS-aware autonomic resource management approach for cloud computing," *Cluster Computing*, vol. 21, no. 2, pp. 1203–1241, 2018.