

Measuring network security in the cloud : A roadmap for proactive defense

Anjani Kumar Singha [§]

Department of Computer Applications

SRM Institute of Science and Technology (Deemed to be University)

Delhi-NCR Campus

Ghaziabad 201204

Uttar Pradesh

India

Shakti Kundu [§]

School of Engineering and Technology Computer Science Engineering

BML Munjal University (BMU)

Gurugram 122413

Haryana

India

Harsh Pratap Singh [†]

Department of Computer Science and Engineering

Sri Vaishnav Vidhyapeeth Vishwavidyalaya

Indore 453331

Madhya Pradesh

India

Lokendra Singh Songare [@]

Department of Computer Science and Engineering

Medicaps University

Indore

Madhya Pradesh

India

[§] E-mail: anjani348@gmail.com

[#] E-mail: shaktikundu@gmail.com

[†] E-mail: drharshprataps@gmail.com

[@] E-mail: lokendra.songare@gmail.com

Pradeep Kumar Tiwari*

*Department of Computer Science and Applications
Vishwanath Karad MIT World Peace University, Pune
Pune 411005
Maharashtra
India*

Abstract

An exhaustive examination and evaluation of hierarchy network security measuring and optimal active defense in the context of cloud computing is provided in this paper. After collecting all the cloud platform's security-related data obtained via evaluation, the pertinent security data is summarized and analyzed to create the cloud platform's safety record index. This index serves as a benchmark for the cloud platform administrators to evaluate the security vulnerabilities associated with their cloud platform. It offers cloud platform administrators a standard against which to assess the security hazards of cloud platforms. We primarily investigate the building of the cloud platform, the building process of the security situational awareness system, and the estimation of the safety circumstance value and use via the cloud platform's security circumstance understanding system, thereby significantly enhancing the cloud platform's stability, security, and dependability. By implementing the approach, the limitations of conventional network security management are circumvented, as the latter is predicated solely on historical data and is incapable of perceiving real-time alterations in the security condition of the system. Concurrently, the anticipated outcomes are incorporated into the imprecise decision-making system's input, enhancing the evaluation's precision. The approach improves the efficiency and efficacy of predicting the network safety situation in real time, augments the algorithm's rate of convergence and prediction precision, and prevents overfitting from occurring. Simulation experiments conducted using the internet network safety posture dataset demonstrate that this research approach exhibits superior learning efficiency and lower prediction error compared to conventional machine learning and other deep learning techniques.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Computer network security, Association rules, Data mining, Security scenarios, Risk assessment.

1. Introduction

Currently, the majority of research on security for the network posture assessment is concentrated around conventional general networks; this includes studies on the details of system security/network safety evaluation model, a network of things security position elements/data acquiring it, examination index framework, as well as evaluation methods,

* E-mail: Pradeeptiwari.mca@gmail.com (Corresponding Author)

which include techniques utilizing identification of patterns, statistical computation, understanding reasoning, and so forth [1]. The current system, however, has unique features when compared to the previous networking environment, including a complicated design, a big network scale, dynamic virtualized management, a layered services model, etc. Attack behavior progressively demonstrates multistage, cooperative, and massive traits. Furthermore, it is imperative to do a systematic study in this field because internal user threat behavior must be considered and only worsens, making the current network security position assessment technologies ineffective. Typically, cloud platform service providers keep resource ownership, usage, and management distinct. Furthermore, the neighborhood, which is not under the control of the user and directly manages the information sources, is isolated from the storage of the data. However, while cloud platforms offer customers physical, logical, and people management, they provide a different degree of control over data access than traditional resource and information management systems. To guarantee an ongoing functioning of cloud structure security, the security safeguarding mechanism of the platform itself requires to be altered and developed. It must transition from a form of passive defense to active defense, from basic detection of intrusions, virus verifying, vulnerability assessment, attack surveillance, defense system safeguarding, etc., to the development of a cloud-based security management system with a danger event understanding function [2]. Applications for cloud platforms-based secure network incident analysis software include attacks on network detection, anomalous event evaluation, anomalies platform safety tracking, and abnormal platforms protection abnormality reporting. Nevertheless, it is difficult to foresee unexpected network security attacks because of the need for efficient monitoring techniques for the highest level network security operations and the inability to efficiently track complicated location-based network safety attacks [3]. Finding the origins of information about threats and cybersecurity assault occurrences is becoming more and more difficult. There currently needs to be established common cloud platform security threat event management platform, integrated large-scale cloud platform protection event knowledge administration center, or network safety threat information exchange platform. For simplicity of supervisors, online computing systems are frequently split into several security domain subsystems [4]. These subcategories offer different purposes and are geographically dispersed. Security protocols among the various subsystems are separate from one another, and secure gateways are put up to allow communication among

the subsystems. There is frequently confidence between two subsystems. The provider of cloud services can accomplish system-wide privacy by protecting every subsystem.

Contribution of Research

- This framework takes into account both quantitative and qualitative metrics, as well as active and passive monitoring techniques. This is important because traditional security metrics, such as firewall throughput and IDS alerts, are no longer sufficient for measuring the security posture of cloud-based networks.
- The article identifies a number of key challenges associated with measuring network security in the cloud. These challenges like the complexity and heterogeneity of cloud environments.
- The article provides a roadmap for implementing proactive defense in the cloud. This roadmap like assess the current security posture of the network.

2. Related Work

The method of evaluating and computing the outcomes of circumstances gathering data is known as circumstance evaluation. Its goals are to give network managers a foundation for making choices, a visual representation of the network's nodes, and a comprehension of its general state. The two main categories of circumstance evaluation techniques are quantitative and qualitative methods [5]. Although qualitative evaluation techniques are more suited for making choices, they can also determine the safety condition of the network as a whole as well as particular nodes, which include additional ones like organizes and services. Qualitative assessment methods are limited in quantifying generate alterations related to network posture [6]. As a result, most professionals and academics have studied the quantitative evaluation of posture in great detail. There is a description of how Markov model games are applied to cyber security awareness of situations techniques [7]. The fusion of multisensory data gathers a set of resources, dangers, and weaknesses, and an attack and defense scenario in the network is described using a reciprocal game of the target's defense, neutrality party, and Markov's state transference property. The evaluation results are more thorough and impartial since the assets, risks, and vulnerabilities are systematically and continuously analyzed [8]. Nevertheless, the process

could be more efficient for large-scale network evaluation since it employs an algorithm that iterates to generate hardening solutions and determine threat posture values, which needs a lot of resources. It is suggested that capability chance intent modeling be applied to cyber security awareness activities apply to them, and all three indices are then integrated to determine the overall security of the network position value [9]. The pace, volume, and arrangement of information generated in the big data era have complicated networks, making it challenging for conventional network security situational(NSS) awareness methods to handle this issue properly. The investigation focuses on big data analysis techniques for the security of the network's situational examination, prediction, and visualization [10]. A network security situational awareness technique for multistep attacks is being explored because of the massive, integrated, and multi-stage features of network attack threats in recent years. This technique effectively helps the decision-making security managers [11]. The research suggests using a situational awareness framework for devices that use edge computing to protect the security of these devices because internet-based edge information technology devices are vulnerable to attacks. This model analyses the system's state at different times to identify possible breaches and provide alerts [12]. In a big data setting, a computer network comprises numerous linked machines, servers, routers, sensors, and other devices. It is an intricate network of data that belongs to an expansive, open system. This complex network of information comprises an enormous amount and variety of subsystems, and there are intricate relationships between them that involve nonlinear behavior, unpredictability, fuzzy thinking, and other factors. Between the external environment and the system, a lot of information is exchanged [13]. The empirical examination of a network's topology, the connection across network function and structure, the development process and evolution law within a network, the relationships between network dynamics and behavior, and the security evaluation of complicated knowledge networks [14]. Gaining a full understanding of the security condition of the cloud platform can only be accomplished by taking into account the multilayer postures of the network layer, virtualized layer, and hosting layer [15]. To increase the accuracy of the postural evaluation algorithm, first, enhance the existing algorithm or create a new one [16]. Then, optimize the algorithm's structure or parameter choice [17]. Second, the model should be built to raise the non-network layer evaluation to enhance the algorithm's thoroughness [18].

3. Cloud Computing Environments: Optimal Active Defense Analysis for Hierarchical Network Security Assessment

3.1 Cloud Architecture for Hierarchical Cybersecurity Measurement

The protection scenario indication serves as the foundation for condition computation and assessment. It is an indication mark that represents the protective characteristics of the viewed object. The main factors affecting security include numerous network threats and assets in the cloud computing setting, which are essential for the whole thing to function. Consequently, vulnerabilities reflect the potential effects of attack threats on resources from the standpoint of the resources themselves. The components of a cloud computing system are assets and relationships among them. Purchases are in danger when vulnerabilities exist, and vulnerabilities will always exist. The risk is taking advantage of an asset's weaknesses to harm it. As a result, it will put the system in danger and impact the computing system's cybersecurity [14]. The three primary characteristics that indicate the degree of security of a resource are accessibility, privacy, and integrity [19]. Threats to assets are evaluated based on how much they affect the security qualities of the purchase rather than how much of its economic worth is lost. The degree of asset security will depend on how easily the threat may exploit the asset's vulnerability and how well safety safeguards are implemented. The security threats in an environment where cloud computing is used are characterized by exposure. The acquisition sustains no harm if the related threat fails to exploit the vulnerability. The danger has no weakness to find and won't result in an incident of security if an exposure is absent from the system. Vulnerabilities can be identified using industry norms, safety guidelines, or international or national security standards [20]. Since the location of a given exposure will change methodologies in Figure 1, it determines the security threat situation for each server's service; raw parameters such as vulnerability information and IDS alarms are merged with network bandwidth.

$$y = \frac{1}{1 - (w^T x + b)} \quad (1)$$

In a logistic regression, the model's characteristics need to be calculated based on a training set of data. The model will produce more accurate predictions and, ultimately, correct categorization with the ideal parameters. Generally speaking, we employ the maximum probability approach to modify the objective function that the leading likelihood

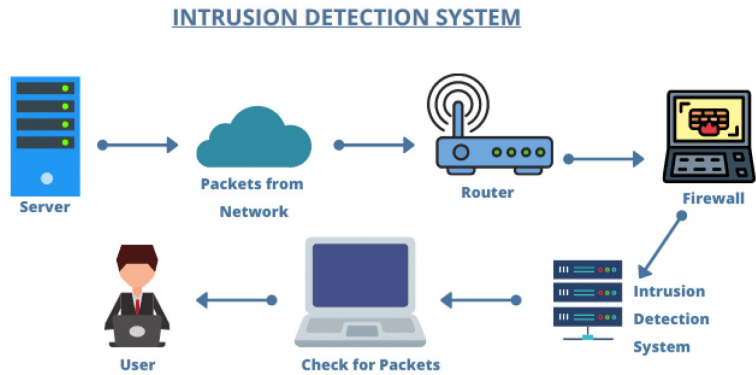


Figure 1
Intrusion detection systems

technique produced using an algorithm for gradient descent and to estimate the logistic regression parameters ω and b , maximizes the chance of logistic regression [15]. By using the great likelihood approach to estimate parameters, the maximum log-likelihood function can be derived.

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

Maximizing (2) is equivalent to minimizing.

$$l(w,b) = \sum_{i=1}^m (x_i w^T . y_i^2 - \ln(1 - e^{-(w^T . y - b)})) \tag{2}$$

Implementing a mathematical model and logistic regression solution is comparatively easy and effective, and it can serve as a useful baseline for further model optimization. Logical regression is an extremely effective classification that handles nonlinear issues by separating and transferring

Table 1
Risk rating matrix

Very rare	Rare	Often	Frequent	Risk probability	Risk impact
<u>Medium</u>	<u>Medium</u>	Medium	High	Medium	Very low
High	Low	High	Medium	Low	Low
High	<u>Medium</u>	High	Medium	Medium	Moderate
Low	High	Low	Medium	High	Serious
Medium	High	Medium	Low	Low	Very serious

data. Therefore, we might use a logistic regression model to remedy the problem when the sample information has a higher concentration of low-level features.

Analyzing the subsequent risk scale matrix, we develop a risk scale with varying implications and probabilities during the risk assessment. We concluded that the decision theory should be applied in the risk evaluation procedure due to the poor data quality and issues with estimating and assessing risks based on historical data. As seen in Table 1, the fuzzy set theory provides a logical approach for application. It also addresses the ambiguity in risk assessment decisions.

This framework promptly identifies hazardous and vulnerable environments, examines weaknesses and vulnerabilities, and detects insecure arrangements at the initial level [18]. By doing so, it effectively accomplishes the objective of fortifying the network environment's security.

3.2 Security Precautions Analysis of Optimal Active Defense

The assessment. Numerous variables may influence the security status of networks in a situation dominated by big data. An evaluation of the network's safety situation will incorporate raw data from various network apparatus, such as knowledge about malicious programs, abnormal traffic, vulnerabilities, and attacks, among others. There is less uncertainty regarding the factors influencing the safety of networks in the context of big data, and a network security state assessment is more comprehensive.. After a series of iterations leading to convergence, the ultimate weight of every vertex is determined. Using the weighting

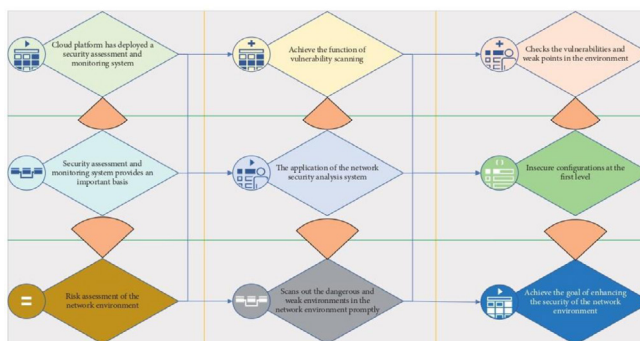


Figure 2

Flowchart of the denial of external network access by a firewall.

procedure, the security position value of the entire network is subsequently determined in show in Figure 2.

4. Analysis of Results

4.1 Evaluation of the Security of Optimal Active Defense Outcomes

In order to mitigate the influence of varying indications on the evaluation outcomes, the parameters are normalized before their integration with the hierarchy analysis approach to derive the parameters reflecting the entire network’s security posture. An increased occurrence of security events signifies a more severe risk that the network is exposed to. A comparison is illustrated in Figure 3 between the posture values computed using the system of metrics. The cloud-based platforms are typically partitioned into numerous sub regions according to the physical setting or host. The Figure 3 and Figure 4 below illustrates an experimental simulation of a three-sub region cloud platform to validate the efficacy of the proposed platform situational fusion algorithm show in Figure 5.

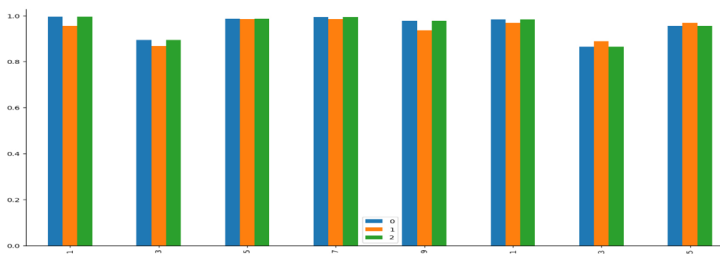


Figure 3
Subset of threat samples.

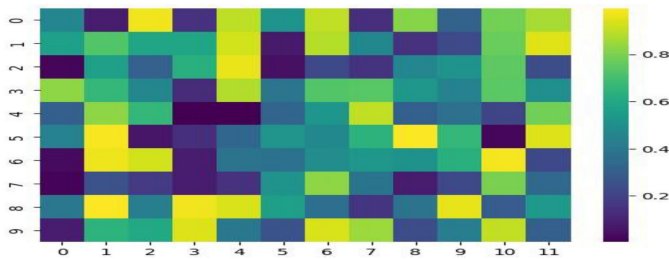


Figure 4

for every danger that was found, the original frequency values, probability values, and recalculated frequency values were obtained.

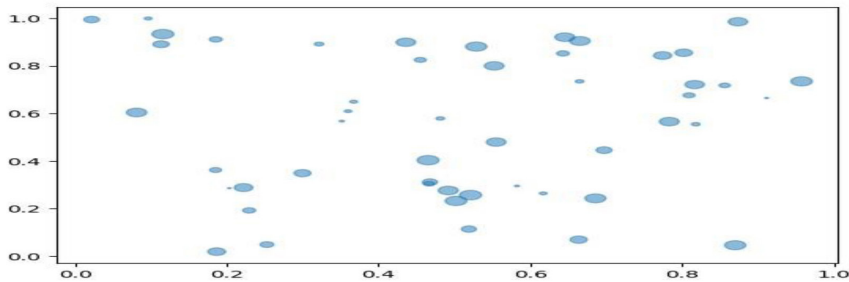


Figure 5

Risk rates for several examples are compared.

4.2 Security Evaluation of Ideal Active Defense Outcomes

To prevent differing indication levels from influencing the findings of the evaluation, each of the indicators is adjusted for normality before being integrated with the multilayered analysis approach to determine the security network position values. To confirm the efficacy of the indication system creation method, the tests performed in this part use the networked domain's safety condition evaluation as an example. In a computer network, the system's security posture can be inferred from the number of security-related events; the higher the number of security events, the greater the danger the network faces. Figure 6 compares the amount of protected data logs in the network platform with the posture values determined by the system of measurements. Graph 8 indicates that the highest and lowest endpoints and the two distinct curve directions were identical, thus suggesting that the indicator system built by clusters in the present research is capable of evaluating the network's security condition. There are fewer security incidents, Based on the technique's evaluation results, the safety situation should have been lower than on February 23. This paper's strategy finds a minimum value point and a maximum value point on became a holiday, there have not been numerous safety concerns on the network. As a result, the most recently recorded lower point was also the computed trending value. In, the first day of classes, there was a massive surge in network traffic. As a result, there were many network security incidents often, and this day's tendency rating was also at its highest. In displays the shifts in the chosen time points. The existing cloud infrastructure is safeguarded if its overall cloud infrastructure posture rating is lower. On the other hand, a greater aggregate cloud platform safety posture indicates an increasingly dangerous status of the present-

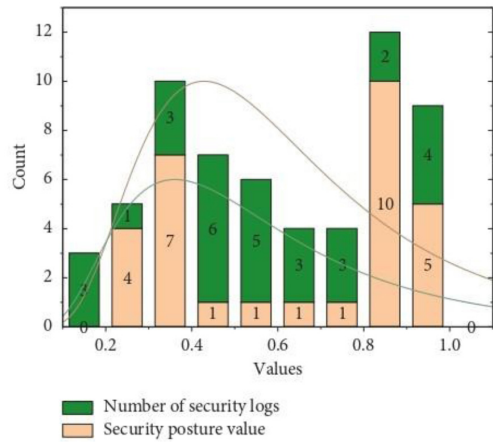


Figure 6
Number of security logs vs Security posture values.

day cloud computing infrastructure. This study proposes developing a cloud-based posture fusion methodology that can precisely reflect system safety posture changes under various operational scenarios. They are less prone to local extremities throughout the iteration, improving training efficiency. The adaptable genetic algorithms offer exceptional global search capabilities and quick optimization. Its selection, crossover, and variance operators can be altered continually based on the total quantity of iterations.

5. Research Gap

The title indicates that the research paper or study intends to address the current state of network security in cloud computing, propose a roadmap for implementing proactive defense strategies, and potentially highlight areas where additional research is necessary. To get a more detailed understanding of the research, you would need to read the full paper or report, as it would likely provide insights into the specific challenges, methodologies, and gaps in the field of cloud network security.

6. Conclusion

Concerning detecting unidentified dangers, the defensive posture assessment model laid out in this article requires improvement. Due to the dynamic and increasingly intricate nature of safety threats, the situational

consciousness model presented in this paper is not capable of forecasting the likelihood of unidentified dangers. This limitation arises from the model's reliance on the danger's incidence module to predict recognized threats. Consequently, efforts can be directed toward forecasting unidentified risks to improve the contextual awareness model's capability to detect such dangers. By applying hierarchical analysis to determine the corresponding weights of comparable evaluation factors, an optimized index system is produced by simplifying the evaluation elements based on the consequences. The results of experiments utilizing data derived from a real academic network environment indicate that the security stance values generated by the approach are capable of precisely capturing modifications in the true security of the network posture.

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] A. K. Singha, S. Zubair, A. Malibari, N. Pathak, S. Urooj, and N. Sharma, "Design of ANN Based Non-Linear Network Using Interconnection of Parallel Processor," *Computer Systems Science & Engineering*, 46(3) (2023).
- [4] S. Zubair, A. K. Singha, N. Pathak, N. Sharma, S. Urooj, and S. R. Larguech, "Performance Enhancement of Adaptive Neural Networks Based on Learning Rate," *Computers, Materials & Continua*, 74(1) (2023).
- [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] R. Mythili, N. Parthiban, and V. Kavitha, "Construction of heterogeneous medical knowledge graph from electronic health records," *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 921–930 (2022).
- [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] R. Gupta, and S. K. Malik, "An analysis of SPARQL usage for information retrieval in heterogeneous domains through various tools," *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1031–1040 (2022).
- [14] A. K. Singha, N. Pathak, N. Sharma, A. Gandhar, S., Urooj, S. Zubair, and G. Nagalaxmi, "An Experimental Approach to Diagnose Covid-19 Using Optimized CNN," *Intelligent Automation & Soft Computing*, 34(2) (2022).
- [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] A. K. Singha, and S. Zubair, "Combination of Optimization Methods in a Multistage Approach for a Deep Neural Network Model," *International Journal of Information Technology*, 1-7(2023).