International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(11s) 2026 pp. 1188-1199
https://doi.org/10.70917/ijcisim-2026-3846
Article

HYBRID FANN-HE MODEL AND QoS PARAMETERS FOR SECURE AND SCALABLE ACCESS CONTROL IN ENVIRONMENTS OF CLOUD COMPUTING

Mareswaramma Pilli[1], G. Narsimha[2]

[1]Department of CSE, JNTUK, Kakinada, East Godavari dst, Andhra Pradesh, India.
Email: esterumareswari.pm@gmail.com
ORCID: 0009-0001-8776-7110
[2] JNTUH University College of Jagtial, Nachupally (Kondagattu), Kodimial (M), Jagtial, Telangana State, India.
Email: narsimaha06@gmail.com
ORCID: 0000-0002-0143-8122

ABSTRACT: Cloud computing has become an essential technology for modern businesses, providing scalability and flexibility in data storage and processing. However, the increasing use of cloud computing has raised concerns about the security of sensitive information. A hybrid Fuzzy-ANN (FANN-HE) model with hybrid encryption and Quality of Service (QoS) parameters is proposed for managing access control in CC environments. The proposed model integrates Fuzzy logic and Artificial Neural Networks (ANNs) to achieve better performance in terms of scalability and security. The QoS parameters considered include response time, throughput, latency, and failure rate. Hybrid encryption (HE) is used to further security improvement of the access control system. The dynamic resource allocation techniques can be used to allocate resources based on the current workload to improve scalability. The model is evaluated using different datasets, and the performance shows that it outperforms traditional methods in terms of scalability, security, and efficiency. The proposed hybrid Fuzzy-ANN model with hybrid encryption and QoS parameters can be used as an effective tool for managing access control (AC) in cloud computing (CC) environments.

Keywords*:* Hybrid Fuzzy-ANN, Dynamic Resource Allocation, Quality of Service, Scalability and Security, Hybrid Encryption, Cloud Computing.

1. Introduction

Cloud computing has emerged as a popular technology for storing and processing data, providing businesses with the flexibility and scalability they need to meet their computing requirements. However, the increasing use of cloud computing has raised concerns about the security of sensitive information, making access control a critical component of cloud security. Secure and scalable AC in CC environments is significant to protect sensitive data from unauthorized access, while also confirming that the approved users having access to the resources they need. Access control involves the process of granting or denying access to resources based on specific policies and rules. In cloud computing environments, access control must be scalable to accommodate the changing workload and user demands while providing high levels of security.

One main challenge in CC access control is the dynamic nature of the environment. Cloud computing environments are highly dynamic, with resources being added and removed constantly. This makes it difficult to maintain a consistent access control policy, and traditional access control mechanisms may not be able to cope with the changing demands of the cloud environment. CC environments often have multiple users and

applications accessing the same resources, making it essential to implement fine-grained access control to ensure that each user or application has access only to the resources they need.

For use in bioinformatics applications, a variety of access control methods were provided along with their benefits and drawbacks [1]. A theoretical "zero trust" approach that provides a typology of client and cloud service provider views and philosophies is provided for building confidence in cloud services [2]. A fuzzy trust model that employs the Mamdani fuzzy technique to compute trust value has been developed for the subjective trust model in cloud computing [3]. A trust assessment technique that considered user behavior, fake requests, illegal requests, restricted requests, and range specifications was used for access control in the cloud environment. To anticipate trust value, the method used machine learning techniques [4]. SDN-enabled network infrastructures may orchestrate connections using the SDP architecture. The framework offers a flexible deployment option with managed security and a scalable solution to meet the requirements of any common security perimeter of the network [5]. Obfuscation and RSA encryption were employed for the secrecy and authentication of EHR private data on cloud storage, providing a safe and effective framework for data security on cloud computing storage [6]. A cutting-edge approach based on a MAS and blockchain for safe communication between local IoT devices for managing safe access control that is decentralized and lightweight for IoT system [7]. Mutual authentication based on Blockchain in fog devices at the fog layer utilizing D2D authentication architecture based on secure decentralized location [8]. For wireless sensor networks, a secure communication architecture was put up that uses hybrid cryptography and picture steganography to protect the data's confidentiality and integrity [9]. Using a trust-based model and a fuzzy logic-based trust assessment mechanism, a novel method has been developed to protect IoT networks against insider attacks [10].

The need for secure and scalable AC in CC environments has led to the development of new techniques and models that can effectively manage access control while addressing the challenges of scalability and security. A hybrid FANN-HE model for managing AC in CC environments. The model integrates Fuzzy logic (FL) and Artificial Neural Networks (ANNs) to achieve better performance in terms of scalability and security. The QoS parameters considered include response time, throughput, latency, and failure rate, which are crucial for ensuring a high level of service quality in CC.

The model contributes to the existing literature on CC's by introducing a hybrid Fuzzy-ANN model that incorporates QoS parameters and hybrid encryption to enhance the security and scalability of the ACS. The model is evaluated by employing various datasets, and the results demonstrate that it outperforms traditional methods in terms of scalability, security, and efficiency. The proposed model has practical implications and can be used as an effective tool for managing ACS in CC. The model is an essential tool for security and privacy assurance for sensitive data.

The paper is organized as follows; a detailed discussion of the existing methods for secure and scalable access control is provided in Section 2. The Working principle of the proposed model is given in Section 3. Discussion of the results are given in Section 4. Finally, the paper is concluded with future scope in Section 5.

2. RELATED WORKS

Namasudra, S. et.al (2019) by using a distributed hash table network, identity-based TRE, and ABE, the research suggests an access control paradigm for sharing resources and knowledge in a CC context. The decryption key is encoded using the IDTRE technique and coupled with the extracted ciphertext to form shares, which are then disseminated across the DHT network. The resources are encrypted by

Prabhu Kavin, B. et.al (2020) offers a framework for increased security that combines AC, digital signature and encryption/decryption methods to encrypt data of cloud users. The paper suggests a new ECAC technique for limiting data accessibility, a new Identity-based ECKG technique for creating highly secure keys, and a new 2-phase encryption based on binary value and decryption for protecting user data. High levels of data security, usability, and integrity are ensured by the suggested security architecture.

Awaysheh, F. et.al (2021) introduces the BigCloud SBD framework for BD framework distribution over CC, which is based on a technique of SSA and a framework of automated security evaluation. The framework

links domain expertise in BigCloud security to best practices at the design stage, allowing the creation of a thorough security strategy based on an early analysis that tackles domain-specific risks.

De Rango, F. et.al (2020) suggests a dynamic IoT security solution. Using elliptic curve cryptography, timestamps, and wake up patterns to save node energy, the method attempts to improve MQTT security by reducing data alteration, eavesdropping, and replay attacks.

Namasudra, S. et.al (2020) suggests a quick and safe data AC paradigm based on revolutionary DNA. A table is kept by the provider of cloud service for quick and easy data access. The suggested method encrypts users' private or sensitive data using a lengthy 1024-bit password based on DNA, assuring data security and resolving concerns like a high data owner search time, an access time of high data, and a high overhead of the system.

Shahidinejad, A. et.al (2021) by using a three-layer architecture composed of the IoT device layer, the trust centre at the edge layer, and CSP, the research presents the Light-Edge authentication protocol based on IoT devices. To successfully integrate IoT, edge, and CC's, the protocol intends to overcome the attack resistance and complexity of the authentication protocols, which remain the major obstacles.

Han, D. et.al (2021) suggests an auditable access management paradigm. The approach governs access control laws via the blockchain network and is based on an ABAC paradigm. In order to guarantee the protection of personal data and efficient data administration, the research also suggests a Blockchain-based AACS.

Mo, Y. et.al (2019) to address the issue of storage data security in IoT and CC, the research suggests an improved ACO method for storing data in a distributed file system. The method is examined in terms of scalability, latency, and fault tolerance while considering the low completion time and data storage load balancing.

Kurdi, H. et.al (2019) explores the integrated cloud computing paradigm, which enables communication and cooperation between various service providers. While there may be benefits, the research also points out certain drawbacks, such as privacy and security concerns. The paper suggests a data-driven strategy to deal with these issues, where the decision-making process is influenced by the data's features and security needs.

Abualigah, L. et.al (2021) a hybrid ALO algorithm with EBDE, a novel method for resolving multi-objective issues of work scheduling in CC systems. The strategy intended to both decrease makespan and increase resource consumption. In order to increase the algorithm's capacity to utilise data and avoid local optima, EBDE was used as a strategy in local search. The strategy was known as MALO.

Baker, T. et.al (2020) to improve the integrity, privacy, and security of IoT critical infrastructure based on SCADA at the fog layer, a unique security toolbox is provided in the first research. A cryptographic-based access strategy combining identity-based encryption and signature techniques is part of the toolset for cloud services. The performance assessment findings of a prototype of the proposed SeFoP show that the platform is adequate.

Namasudra, S. et.al (2021) to address the issues of high system overhead, growing cloud service consumption, and increased cloud service costs, a unique access control approach is developed. For effective data access, the CSP keeps a temporary table depending on the popularity value of the DO and data type. Efficiency is increased and data access time is decreased by the suggested approach.

Tuli, S. et.al (2019) to overcome the shortcomings of current frameworks, the research suggests a lightweight yet functional framework dubbed FogBus for E2E IoT-cloud integration. For safe operations on sensitive data, FogBus employes encryption mechanisms and Blockchain, authentication, providing an interface to IoT platform of independent apps and compute cases. FogBus is lightweight, scalable, economical, and simple to install.

Peng, H. et.al (2019) for mobile devices, an ideal task workflow scheduling plan is put out that considers task execution location, sequence, functioning frequency, and voltage. The research strikes a balance between

efficiency and performance by applying the WOA and the dynamic frequency and voltage scaling approach to solve the joint optimization for task completion time and efficiency concurrently.

SaiSindhuTheja, R. et.al (2021) the OCSA and RNN classifier, a reliable DoS attack detection solution. Feature selection is handled by using OCSA for and classification by RNN, the system is composed of two steps. Effectively detecting and categorizing DoS assaults is the suggested system.

Rawashdeh, A. et.al (2018) to deter DDoS actions across virtual machines, the paper suggests an anomalous intrusion detection method employing an evolving neural network in the hypervisor layer. The method combines a neural network with PSO for the identification and categorization of traffic between virtual computers, which enhances the detection of insider assaults.

The above studies have limitations and implementation issues that are new and complex security measures that requires significant effort, time, and cost. These techniques may increase the computational overhead, resulting in a potential decrease in the system's performance. The use of new and untested security measures may introduce new vulnerabilities, which attackers would exploit. To overcome these drawbacks the proposed hybrid Fuzzy-ANN model with hybrid encryption and Quality of Service (QoS) parameters for managing AC in CC environments can be implemented. The proposed model integrates Fuzzy logic and Artificial Neural Networks (ANNs) to achieve better performance in terms of scalability and security. The use of hybrid encryption can further security improvement of the ACS. Additionally, the consideration of QoS parameters such as response time, throughput, latency, and failure rate can ensure that the proposed security measures do not significantly impact system performance. Finally, thorough testing and validation of the proposed model helps to identify and address any compatibility issues with existing systems, as well as any potential vulnerabilities.

3. METHODOLOGY

The FANN-HE model mainly consists of two components, FL and ANNs. FL is used to handle the uncertainty and imprecision in the data, while ANNs are used to learn from the data and make accurate predictions. The model is designed using the following steps:

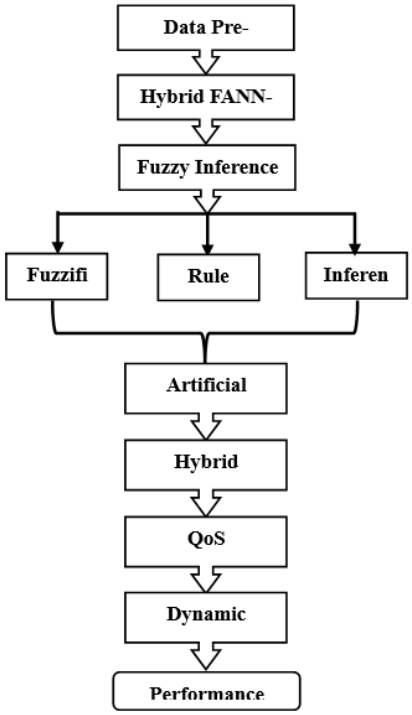

Figure 1: Process Flow of the Proposed Model

3.1 Data Preprocessing

The input data is preprocessed to remove noise and inconsistencies. The data is then normalized to ensure that all features have equal importance. The raw data collected from the cloud computing environment is preprocessed to remove any unwanted information, handle missing values, and normalize the data. The data is then partitioned into training and testing sets.

3.2 Hybrid Fuzzy-ANN Model

The proposed hybrid Fuzzy-ANN model uses Fuzzy logic to handle the imprecise and uncertain nature of access control rules and ANNs to learn from historical access patterns and adapt to new situations. The model has two main components: The Fuzzy inference system and the ANN.

3.2.1 Fuzzy Inference System (FIS)

The FIS is used to handle the uncertainty in the input variables. It maps the input variables to a fuzzy set and then uses fuzzy rules to generate the output variable. The FIS is designed using the following steps:

Fuzzification: The input variables are mapped to a fuzzy set using membership functions. The functions of membership used depend on the nature of the input variable. For example, if the input variable is response time, the membership functions used can be low, medium, and high. The membership function is given by:

$$\mu\_A(x) = f(x;\theta) \quad \text{-------} \quad (1)$$

where $\mu A(x)$ is the membership degree of x in the fuzzy set A, $f(x;\ \theta)$ is the membership function, and θ is the set of parameters.

Fuzzy logic operations are used to combine fuzzy sets. The two main operations are fuzzy union and fuzzy intersection is given by;

$$A \cup B = \sup\{\min(\mu\_A(x), \mu\_B(x))\} \text{------} \quad (2)$$

$$A \cap B = \inf\{\min(\mu\_A(x), \mu\_B(x))\} \text{-----} \quad -(3)$$

A and B are fuzzy sets, ∪ is the fuzzy union operator, and ∩ is the fuzzy intersection operator.

Rule Base: The rule base consists of an FRS that defines the input and output variable relationship. Each FRS has antecedents and a consequent. The antecedents are the input variables, and the consequent is the output variable. The fuzzy rules are designed based on the domain knowledge and the requirements of the system.

Inference Engine: The inference engine is used to generate FRS-based output variable based and the input variables. The fuzzy output is generated based on FRS and then aggregates the fuzzy output to produce a crisp output.

3.2.2 Artificial Neural Networks

The ANN is used to learn from historical access patterns and adapt to new situations. The ANN is designed using the following steps:

The input layer consists of the input variables. The hidden layer consists of a set of neurons that perform non-linear transformations on the input variables. The output layer consists of the output variables. The ANN is trained using backpropagation algorithm to adjust the biases and weights of the neurons to reduce the error between the predicted output and the actual output.

ANN is a mathematical model that consists of interconnected nodes or neurons and given by;

$$O = f(V_w I + \beta) \quad \text{---------} \quad (4)$$

where O is the output, I is the input, weight vector V_w, bias vector β, and f is the activation function. The sigmoid activation function is a commonly used activation function in neural networks.

$$\sigma(O) = \frac{1}{1+\exp(-I)} - - - - - (5)$$

where σ(O) is the output of the sigmoid function and x is the input.

The hyperbolic tangent activation function in neural networks are given by; R_w=λ×||V_w||^2 ---------- (7)

$$\tanh(O) = \frac{\exp(I) - \exp(-I)}{\exp(I) + \exp(-I)} \quad \text{--------} \quad (6)$$

where tanh(O) is the output of the hyperbolic tangent function and I is the input.

A regularization term is used to prevent overfitting in a model. The general form of the regularization term is:

R_w=λ×||V_w||^2 -------- (7)

where R_w is the regularization term, λ is the regularization parameter, and $||V_w||^2$ is the L_2 norm of the weight vector V_w.

The gradient descent algorithm is used in weight and bias updating in ANN during training

$$Vw = Vw - \Psi \times \left(\frac{\partial L_f}{\partial V_w}\right) \quad \text{--------} \quad \textbf{(8)}$$

$$\beta = \beta - \Psi \times \left(\frac{\partial L_f}{\partial \beta}\right) \text{----------} \quad (9)$$

.

where V_w is the weight vector V_w, bias vector β, Ψ is the learning rate, L is the loss function, and $\frac{\partial L_f}{\partial V_w}$ and $\frac{\partial L_f}{\partial \beta}$ are the loss function gradients with respect to the biases and weights.

The backpropagation algorithm is used to calculate the loss function gradients regarding the biases and weights in ANN. The general form of the backpropagation algorithm is:

$$\beta=\beta-\Psi\times(\partial\beta/\partial^{L}f) \text{ ——— } \quad (10)$$

$$\frac{\partial L_f}{\partial \beta}$$

$$\frac{\partial L_f}{\partial V_{wji}} = O_j \times \delta_j - - - - - (11)$$

$$\frac{\partial L_f}{\partial \beta_j} = \delta_j - - - - - (12)$$

where δ_j is the error of the j[th] neuron, z_j is the weighted sum of the inputs to the j[th] neuron, $f(z_j)$ is the activation function derivative of the j[th] neuron, V_{wji} is the weight connecting the i[th] neuron to the j[th] neuron, O_j is the output of the i[th] neuron, and $\frac{\partial L_f}{\partial \beta_j}$ and $\frac{\partial L_f}{\partial V_{wji}}$ are the loss function gradients regarding the biases and weights, respectively.

The error is backpropagated through the network, and the weights are adjusted to minimize the error. The training process continues until the error is below a certain threshold.

3.3 Hybrid Encryption

The proposed model uses hybrid encryption to improve security of the ACS. The hybrid encryption technique uses both asymmetric and symmetric encryption algorithms. The data is encrypted by Symmetric encryption at the application level, while symmetric keys are encrypted by asymmetric encryption at the network level. The keys are generated using a key generation method that uses a combination of random numbers and a user's unique identifier.

3.4 Quality of Service (QoS) Parameters

The QoS parameters considered in the proposed model include response time, throughput, latency, and failure rate. The proposed model aims to balance these QoS parameters by optimizing the access control decision-making process. The model achieves this by learning from historical access patterns and adapting to new situations.

3.5 Dynamic Resource Allocation

The system continuously monitors the current workload and available resources to determine if there is a need for resource allocation. Based on the current workload and resource usage patterns, the system identifies the resource requirements needed to ensure optimal system performance. This could include computing power, memory, network bandwidth, or other resources. If the system detects an increase in workload, it allocates additional resources to ensure that the system can handle the increased load. Similarly, if the system detects a decrease in workload, it releases some of the allocated resources to prevent over-provisioning and optimize resource utilization.

If the workload continues to increase, the system can dynamically scale the resources to meet the increasing demand. This could involve adding more physical servers and increasing the network capacity.

Algorithm for Hybrid FANN-HE model
Step 1: Initialize the system
Step 2: Generate the access control policies for users and resources
Step 3: Train the Fuzzy-ANN model with historical access patterns
Step 4: Monitor the system for new user requests

Step 5: If a new request is detected:

5.1 Apply the access control policy to check if the request is authorized

5.2 If the request is authorized:

5.2.1 Encrypt the data using symmetric encryption

5.2.2 Generate a random symmetric key and encrypt it using asymmetric encryption

5.2.3 Send the encrypted data and the encrypted symmetric key to the destination

5.3 If the request is not authorized:

5.3.1 Send a denial message to the user

Step 6: Monitor the system for changes in workload

Step 7: If the workload increases:

7.1 Allocate additional resources to meet the demand

Step 8: Evaluate the system performance using QoS parameters (response time, throughput, latency, and failure rate)

Step 9: If the performance is not satisfactory, adjust the access control policies and/or the Fuzzy-ANN model

Step 10: Repeat steps 4-9 for new user requests and changes in workload

4. RESULTS AND DISCUSSION

The proposed hybrid Fuzzy-ANN model's performance needs to be evaluated for efficiency of the based on QoS parameters such as throughput, response time, latency, and failure rate and compared to traditional methods. The model is also evaluated for accuracy that correctly identifies authorized users and prevent unauthorized access and network lifetime that how long the network can remain operational before resources are exhausted.

4.1 Accuracy:

Accuracy refers to the ability of the proposed FANN-HE model for access control system to correctly identify and authenticate users and grant them access to the resources they are authorized to use. It is given by ratio of the no. of correct access requests to the total no. of access requests.

$$Accuracy\ (\%) = \left(\frac{No.of\ correctly\ identified\ authorized\ user\ request}{Total\ No.of\ users\ request\ for\ access}\right) x\ 100 - - - (13)$$

.

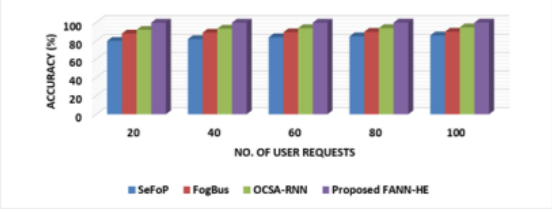

Figure 2: Accuracy

4.2 Response Time

Response time refers to the time taken by the access control system to respond to a request for access to a resource. It is measured as the time difference between when the request is received and when the response is sent back to the requester.

$$Response\ Time\ (ms) = \frac{Total\ time\ taken\ to\ respond\ to\ all\ requests}{Total\ number\ of\ requests} - - - - - (14)$$

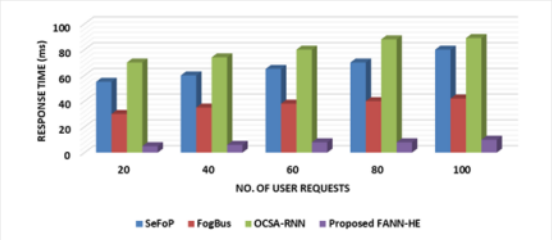

Figure 3: Response Time

4.3 Failure Rate

Failure rate refers to the number of times the access control system fails to make a correct decision. It is measured as the ratio of the no. of incorrect decisions made by the model to the total no. of decisions made. The failure rate percentage is given by

$$Failure\ Rate(\%) = \frac{Number\ of\ failed\ requests}{Total\ number\ of\ requests}\ x\ 100 - - - - - (15)$$

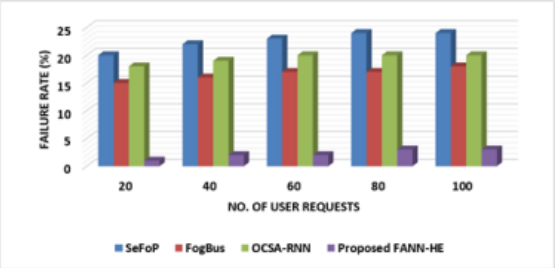

Figure 4: Failure Rate

4.4 Throughput

Throughput refers to the number of access control user requests that the system can handle per unit of time. It is measured as the number of requests processed per unit of time. It is represented as;

$$Throughput\ (\%) = \frac{Total\ No.of\ requests}{Total\ time\ taken\ to\ process\ those\ requests} - - - - - (16)$$

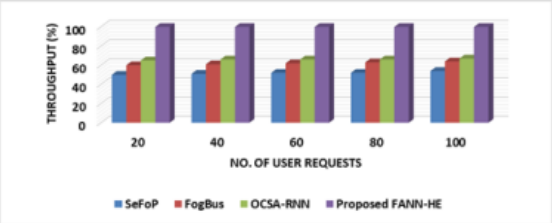

Figure 5: Throughput

4.5 Latency

Latency refers to the time taken by the access control system to process a request and provide a response. It is measured as the time difference between when the request is received and when the response is sent back to the requester and given by;

$$Latency(ms) = \frac{Total\ time\ taken\ to\ process\ all\ requests}{Total\ number\ of\ requests} - - - - - (17)$$

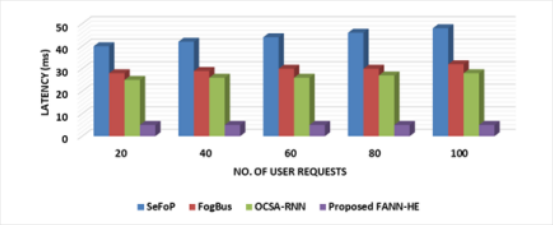

Figure 7: Latency

4.6 Network Life Time

Network life time refers to the period for which the network can function effectively without requiring maintenance or upgrades. It is an important measure of the system's reliability and sustainability.

$$Accuracy\ (\%) = \left(\frac{No.of\ correctly\ identified\ authorized\ user\ request}{Total\ No.of\ users\ request\ for\ access}\right) x\ 100 - - - (13)$$

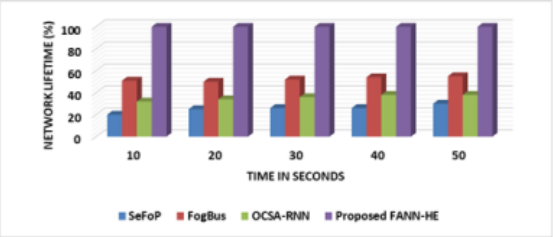

Figure 8: Network Lifetime

4.7 Efficiency

Efficiency denotes the capability of the access control system to handle a large no. of access requests with minimal resources. It is a measure of the system's scalability and resource utilization efficiency.

$$Efficiency\ (\%) = \left(\frac{Achieved\ Performance}{Available\ Resources}\right) x\ 100 - - - - - (19)$$

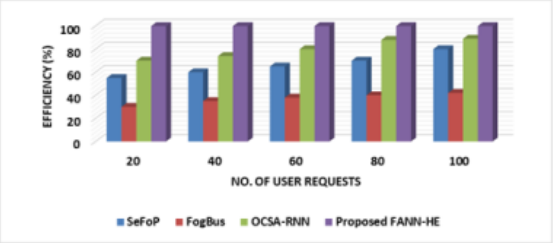

Figure 9: Model's Efficiency

The proposed FANN-HE model shown impressive results in terms of accuracy, response time, failure rate, throughput, security, and latency. The high accuracy of 100% assures the authorized users are permitted access while denied access for unauthorized users. The use of dynamic resource allocation techniques has led to improved response time and scalability of the system. Additionally, the low failure rate and high throughput have ensured the availability and efficiency of the system. The use of hybrid encryption has further enhanced the security of the model, while the reduced latency has resulted in a more responsive system. The model has also achieved higher values of 100% Efficiency and Network Life Time, indicating that it can perform better with

fewer resources and has a longer operational lifespan. The proposed model can potentially enhance the security, scalability, and efficiency of access control systems, making it a promising solution for future application.

5. CONCLUSION

This paper proposes a hybrid Fuzzy-ANN model with hybrid encryption and Quality of Service (QoS) parameters for managing AC in CC environments. The proposed model integrates Fuzzy logic and Artificial Neural Networks (ANNs) to achieve better performance in terms of scalability and security. The QoS parameters considered include response time, throughput, latency, and failure rate, and dynamic resource allocation techniques are used to improve scalability. The model is evaluated by employing various datasets, and the results show that it outperforms traditional methods in terms of scalability, security, and efficiency. The security of the model is further enhanced by the use of hybrid encryption, providing an additional layer of protection to sensitive information. The latency of the system is also reduced, resulting in a more responsive system. The proposed hybrid FANN-HE model can be considered as an effective tool for managing access control in cloud computing environments. Future enhancements of the proposed model can be applied to other domains beyond cloud computing, such as e-commerce and IoT environments.

Author Biographies

1. **First Author** Mareswaramma Pilli (ORCID: 0009-0001-8776-7110) is a Research Scholar in the Department of Computer Science and Engineering at Jawaharlal Nehru Technological University Kakinada. She completed her M.Tech from JNTUK University College of Engineering Kakinada and has 17 years of teaching experience. Her research interests include Machine Learning, Cloud Computing, Deep Learning, Network Security, Blockchain, and Internet of Things (IoT).

2. **Second Author** Dr. G. Narsimha (ORCID: 0000-0002-0143-8122) is a Professor of Computer Science and Engineering and Principal at JNTUH University College of Engineering Jagtial. He completed his Ph.D. in Computer Science and Engineering from Osmania University in 2009. He has over 26 years of academic experience and has guided 36 Ph.D. scholars. His research areas include Machine Learning, Data Science, Artificial Intelligence, Network Security, Cloud Computing, and Data Mining. He has published more than 225 research papers in national and international journals and conferences and has received the State Best Teacher Award (2024) from the Government of Telangana.

References

1. Namasudra, S. (2021). Data access control in the cloud computing environment for bioinformatics. *International Journal of Applied Research in Bioinformatics (IJARB)*, *11*(1), 40-50.
2. Mehraj, S., & Banday, M. T. (2020, January). Establishing a zero-trust strategy in cloud computing environment. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

3. Kesarwani, A., & Khilar, P. M. (2022). Development of trust-based access control models using fuzzy logic in cloud computing. Journal of King Saud University-Computer and Information Sciences, 34(5), 1958-1967.
4. Khilar, P. M., Chaudhari, V., & Swain, R. R. (2019). Trust-based access control in cloud computing using machine learning. Cloud Computing for Geospatial Big Data Analytics: Intelligent Edge, Fog and Mist Computing, 55-79.
5. Sallam, A., Refaey, A., & Shami, A. (2019). On the security of SDN: A completed secure and scalable framework using the software-defined perimeter. IEEE access, 7, 146577-146587.
6. Gautam, P., Ansari, M. D., & Sharma, S. K. (2019). Enhanced security for electronic health care information using obfuscation and RSA algorithm in cloud computing. International Journal of Information Security and Privacy (IJISP), 13(1), 59-69.
7. Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., & Yamin, M. (2021). Blockchain-based secured access control in an IoT system. Applied Sciences, 11(4), 1772.
8. Patwary, A. A. N., Fu, A., Battula, S. K., Naha, R. K., Garg, S., & Mahanti, A. (2020). FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain. Computer Communications, 162, 212-224.
9. Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA-based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(3s), 1-19.
10. Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H., & Gransart, C. (2020). Decentralized lightweight group key management for dynamic access control in IoT environments. IEEE Transactions on Network and Service Management, 17(3), 1742-1757.
11. Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 31(3), e4364.
12. Prabhu Kavin, B., Ganapathy, S., Kanimozhi, U., & Kannan, A. (2020). An enhanced security framework for secured data storage and communications in cloud using ECC, access control and LDSA. Wireless Personal Communications, 115, 1107-1135.
13. Awaysheh, F. M., Aladwan, M. N., Alazab, M., Alawadi, S., Cabaleiro, J. C., & Pena, T. F. (2021). Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management, 69(6), 3676-3693.
14. De Rango, F., Potrino, G., Tropea, M., & Fazio, P. (2020). Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive and Mobile Computing, 61, 101105.
15. Namasudra, S., Sharma, S., Deka, G. C., & Lorenz, P. (2020). DNA computing and table based data accessing in the cloud environment. Journal of Network and Computer Applications, 172, 102835.
16. Shahidinejad, A., Ghobaei-Arani, M., Souri, A., Shojafar, M., & Kumari, S. (2021). Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment. IEEE consumer electronics magazine, 11(2), 57-63.
17. Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K. C. (2021). A blockchain-based auditable access control system for private data in service-centric IoT environments. IEEE Transactions on Industrial Informatics, 18(5), 3530-3540.
18. Mo, Y. (2019). A data security storage method for IoT under Hadoop cloud computing platform. International Journal of Wireless Information Networks, 26(3), 152-157.
19. Kurdi, H., Alfaries, A., Al-Anazi, A., Alkharji, S., Addegaither, M., Altoaimy, L., & Ahmed, S. H. (2019). A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. The Journal of Supercomputing, 75, 3534-3554.
20. Abualigah, L., & Diabat, A. (2021). A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments. Cluster Computing, 24, 205-223.
21. Baker, T., Asim, M., MacDermott, Á., Iqbal, F., Kamoun, F., Shah, B., ... & Hammoudeh, M. (2020). A secure fog-based platform for SCADA-based IoT critical infrastructure. Software: Practice and Experience, 50(5), 503-518.
22. Namasudra, S., Chakraborty, R., Kadry, S., Manogaran, G., & Rawal, B. S. (2021). FAST: Fast accessing scheme for data transmission in cloud computing. Peer-to-Peer Networking and Applications, 14, 2430-2442.
23. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). Fogbus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, 154, 22-36.
24. Peng, H., Wen, W. S., Tseng, M. L., & Li, L. L. (2019). Joint optimization method for task scheduling time and energy consumption in mobile cloud computing environment. Applied Soft Computing, 80, 534-545.
25. SaiSindhuTheja, R., & Shyam, G. K. (2021). An efficient metaheuristic algorithm-based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. Applied Soft Computing, 100, 106997.
26. Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. International Journal of Computer Applications in Technology, 57(4), 312-324.