**International Journal of Data Informatics and Intelligent Computing (IJDIIC)**
Vol. 4, No. 3, September 2025, pp. 41~51
DOI: 10.59461/ijdiic.v4i3.221

# Novel Deep Learning Framework for Automated Access Control in Cloud Computing Environments

**Aditya Gupta[1], Sai Kiran Oruganti[1]**
[1]Department of Computer Science and Engineering, Lincoln University College, Malaysia

**Article Info**

***Article history:***

Received July 20, 2025
Revised September 11, 2025
Accepted September 19, 2025

***Keywords:***

Deep learning
Malleable Clouded Leopard-tuned Deep Recurrent Neural Network
Cloud Computing Environment
User behaviour
Access control

**ABSTRACT**

The rapid adoption of Cloud Computing (CC) has significantly increased the complexity of managing secure and efficient access control due to the dynamic nature of cloud environments. Traditional methods, such as static rule-based systems or Machine Learning (ML) models, often fail to adapt to evolving user behavior and the emerging threats. To address these challenges, a novel Malleable Clouded-Leopard tuned Deep Recurrent Neural Network (MCL-DRNN) is designed for automated, real-time access control and resource allocation in CC environments. This framework utilizes cloud access logs, user behavior metrics, device identifiers, geolocation, time-stamps, and environmental variables. Preprocessing includes data cleaning, normalization, and dimensionality reduction using Principal Component Analysis (PCA) to retain critical patterns. The DRNN model is optimized using the MCL method, enabling the system to anticipate complex access patterns and detect deviations from normal behavior. By leveraging the recurrent structure of the DRNN, the system identifies subtle, persistent abnormalities indicative of potential security concerns. Performance evaluations demonstrate that the MCL-DRNN achieves 95% precision, 96% recall, and 95.6% F1-Score, outperforming traditional approaches. The intelligent, adaptive system provides a robust, self-optimizing solution for enhanced cloud security, capable of adjusting to rapidly changing cloud environments and mitigating unwanted access.



**Corresponding Author:** Aditya Gupta (e-mail: gupta.aditya56@gmail.com)

## 1. INTRODUCTION

As a security measure, access control ensures that only official entities, subject to a set of access control system, can dependably access resources. Access control creates a selective access restriction, which limits who can access something or what can be accessed under particular conditions [1]. Using the internet to supply various services is known as Cloud Computing (CC). Applications and technologies, including databases, servers, networking, software, and data storage, are examples of these resources. Organizations and companies can lease access to storage or processing resources provided by the cloud service instead of owning the data centers or computer tools [2]. CC facilitates virtual collaboration by allowing users to remotely access resources from any location. Unlike old hardware-based computer systems, which took a long time to upgrade resources, CC allows users to do so very rapidly. The issue of excess and underutilization can be lessened with the help of proper resource use [3]. The quick development of CC has completely changed how businesses handle, store, and retrieve data. Nevertheless, the transition to multi-cloud environments has also brought forth new privacy and trust issues. Cloud service providers can't always ensure user data security and privacy, which raises questions regarding data breaches, illegal access, and compliance issues [4]. In recent times, CC has become known as a highly developed field of computer technology that allows for the scalable and cost-effective expansion of computing services. Through CC, users can pay for the resources used, allowing them to request more or fewer resources as needed [5]. Cloud storage is one of the CC services that can offer the ability to store data remotely. Cloud strongly attempts to abstract away the load of managing and maintaining hardware. With CC, Information Technology (IT)

capabilities are dynamically increased without the need for additional software licenses, infrastructure, or staff training [6]. Communication with transportation systems and travel has been totally changed by the Intelligent Transportation Systems (ITS). The ITS effortlessly integrates state-of-the-art technologies to increase the efficiency, safety, and sustainability of transport [7].

### 1.1. Research objective

The Malleable Clouded-Leopard tuned Deep Recurrent Neural Network (MCL-DRNN) will be used in this research to offer a self-optimizing, intelligent, and real-time access control structure for CC environments. The proposed algorithm seeks to enhance detection flexibility, scalability, and accuracy by optimizing the DRNN using the MCL technique.

The outline of the research is organized as follows: Section 2: related work, Section 3: methodology, Section 4: results and discussion, Section 5: conclusion.

## 2. RELATED WORK

The research [8] examined how organizations were adjusting to CC technology. The research also provided a thorough examination of cutting-edge cloud computing approaches. Along with the possible difficulties and limitations that could arise when incorporating CC into corporate environments, the characteristics and methods of delivery of CC were examined. A Genetic Algorithm (GA)-based paradigm called CryptoGA [9] was put up to solve privacy and data integrity concerns. The encryption and decryption keys were generated using GA and combined with a cryptographic technique to keep the integrity and confidentiality of cloud data. The developed model protected privacy against unnecessary access and retained data reliability, based on experimental results.

The improved algorithm proposed [10] a deployment of the Big Data framework over cloud computing (BigCloud), which required the development of a unique security-by-design framework. A completely mechanical safety evaluation structure and a methodical approach to security analysis were its mainstays. The outcomes showed victory in cutting down on security design time and improving safety awareness. The need to utilize contemporary technology, like big data frameworks, CC, and Machine Learning (ML), was underlined [11] to enhance data lakes' potential. Through the adoption of data lakes, businesses were able to expose meaningful insights to increase operational efficiency and achieve innovation and data assets.

The application of Artificial Intelligence (AI)-driven Zero Trust Security models in retail cloud systems was analyzed [12]. AI was used to automate threat prevention, continuous authentication, and anomaly detection in order to implement a sophisticated Zero Trust system. Its effectiveness was examined in comparison to conservative perimeter-based security methods using case studies and simulations to demonstrate how AI improved access control, data protection, and identity verification in contemporary retail cloud environments. The research explored [13] how CC and AI could collaborate to develop cloud services in domains like security, autonomous scalability, and resource efficiency. Intelligent data management, predictive maintenance, and automated cloud operations were just a few of the important use cases and applications that were explored. The research discussed the technical use of AI in cloud systems, going over well-known frameworks, industry best practices, and actual cases.

The method developed in [14] mitigated the issues by integrating blockchain security architecture with AI. At the edge, AI-driven threat intelligence and anomaly detection models were implemented, offering real-time protection against online attacks. Blockchain-based authentication protected data integrity and stopped tampering by improving access control and identity verification. Additionally, federated learning made it possible to share threat intelligence in a decentralized manner, which enhanced cybersecurity cooperation in cloud environments. The algorithm presented [15] a thorough analysis covering a wide range of Autonomous vehicles (AV)-related topics, including international standards, safety and security, environmental effects, public health, social consequences, traffic management, driverless city design, public acceptance, and safety. Furthermore, new technologies, like CC integration, solar power use in driverless cars, and AI, were discussed. Parallel Multi-Key Encryption Algorithm (EPM-KEA) [16] was improved to enhance healthcare data security and facilitate safe cloud storage of critical patient records. The two categories from which the data were collected were Authorization for High Complexity Operations and Authorization for Hospital Admission (AIH). The method presented in [17] used facial and fingerprint biometrics using a Convolutional Neural Network (CNN), extracting features and identifying patterns for secure organization, and used multimodal biometrics to make a non-intrusive cryptographic key for encrypting and decrypting client-uploaded data in the cloud [18].

## 3. METHOD

The proposed MCL-DRNN system (Figure 1) starts by using automated monitoring tools to gather cloud access data, such as time-stamps, device IDs, geolocation, and user behavior. Data cleaning, normalization, and dimensionality reduction using PCA are all part of preprocessing to preserve important patterns. To improve anomaly detection, a DRNN is built to learn temporal access habits and tuned using the MCL approach.

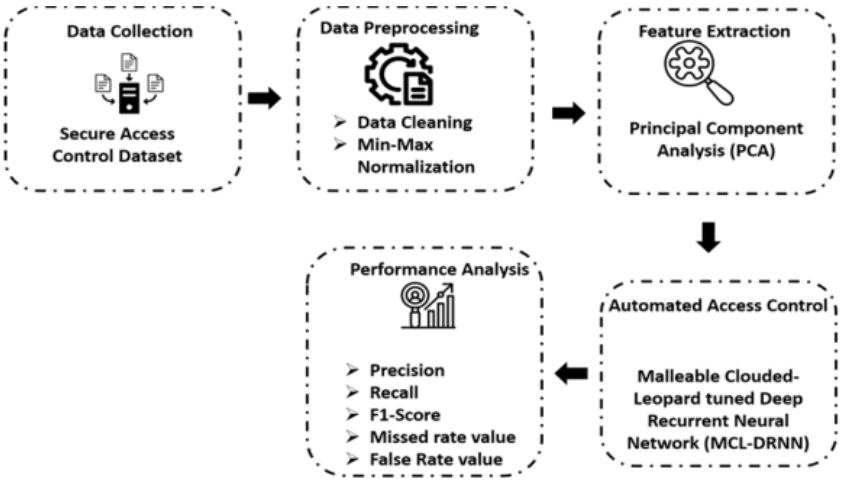


Figure 1. Suggested MCL-DRNN method framework

### 3.1. Data Collection

The dataset analyzes security risks and identifies anomalies by combining access control files from CC and the Internet of Things (IoT) healthcare system. Along with integrating behavioral data from gesture-based activities, the dataset records user interactions, device operations, and security setups (https://www.kaggle.com/datasets/programmer3/secure-access-control-dataset).

Preprocessing involves data cleansing, normalization, and dimensionality reduction using Principal Component Analysis (PCA), which improves feature relevance and reduces computing complexity while keeping critical patterns for anomaly identification. Table 1 shows the description of the dataset features.

Table 1. Feature of the dataset

| Features | Descriptions |
|---|---|
| IoT Healthcare Access Logs | Tracks patient data interactions, sensor readings, and role-based access patterns |
| Cloud Computing Access Logs | Logs authentication attempts, device metadata, and security settings |
| Security Attributes | Includes VPN usage, firewall status, encryption methods, and multi-factor authentication indicators |
| Gesture & Activity Data | Collected from 100 participants performing 10 different gestures and activities, each recorded over a 60-second duration, to analyze behavioral variation. |
| Anomaly Detection | The Target column (1 = Anomalous Access, 0 = Normal Access) labels suspicious activities based on deviations from expected access patterns. |

### 3.2. Automated Access Control in Cloud Computing Environments Using Malleable Clouded-Leopard tuned Deep Recurrent Neural Network (MCL-DRNN)

The proposed algorithm, MCL-DRNN, combines sequential adaptive optimization, modelling, and DL to develop cloud access management. To provide accurate unusual analysis, a recurrent-based feature extraction technique analyzes the access pattern. DRNN hyperparameters are optimized using MCL tuning, which improves detection adaptability and precision. Real-time security threat mitigation is made possible by the DRNN component, which recognizes temporal relationships in cloud access data [19].

### 3.2.1. Recurrent Neural Network (RNN)

The ability of a simple RNN to maintain data in the form of hidden states over time steps makes it a basic type of RNN. A simple RNN's mathematical formulation is as follows in Equations (1 and 2).

$$g_i = \sigma\left(X_{gg} g_i - 1 + X_{wg} w_i + a_g\right) \quad (1)$$

$$t_i = \sigma\left(X_{gt} g_i + a_i\right) \quad (2)$$

Where $t_i$ denotes that time step, $w_i$ is the hidden state, $w_i$ is the input at time step $g_i$, $a_g$ and $a_i$ are weight matrices and bias vectors of $X_{gg}$, $X_{wg}$, $X_{gt}$, whereas $\sigma$ represents the activation function.

### 3.2.2. Deep Recurrent Neural Network (DRNN)

A single-layer RNN, though deep along the time steps because it is sequential, has only one hidden layer when it is unfolded, restricting it to capture intricate temporal relationships and subtle patterns in user behavior. The infrastructural limit makes single-layer RNNs comparatively shallow in information processing. The DRNN's overall architecture is shown in Figure 2, where two DRNN processes access request sequences based on dynamic contextual dependencies, separated by critical event triggers. For accurate, real-time access control decisions in cloud environments, the architecture uses four information channels: device identifiers, geolocation data, access time-stamps, and user behavior metrics. These inputs are encoded and learned over time.

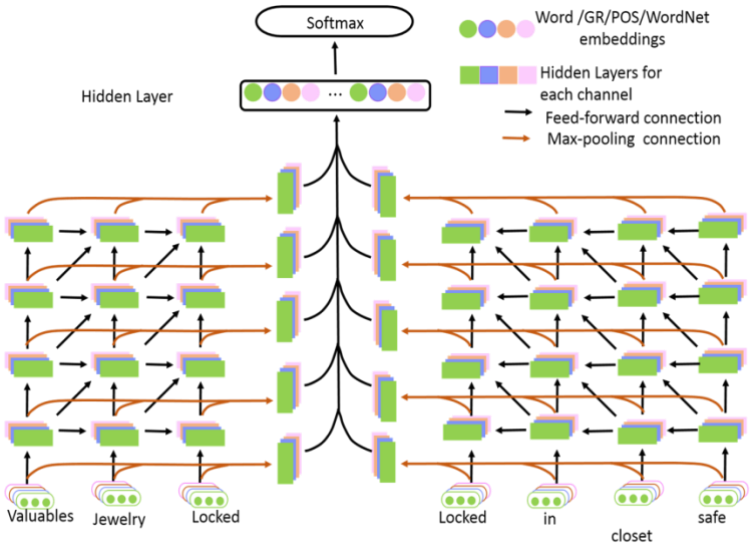


Figure 2. Architecture of DRNN

Different points of view are provided by features along sequential access patterns in the context of real-time access control. Device IDs and geolocation are examples of user-specific features that are intrinsically informative. Conversely, contextual factors that show how these features interact to affect access decisions include behavioral tendencies and temporal patterns. It's possible that this multi-dimensional and heterogeneous data calls for a more intricate layout than a single-layer RNN. By stacking several recurrent hidden layers, the DRNN architecture achieves the goal. Each layer receives input from the one before and determines its activation based on the temporal modeling function, allowing for greater abstraction and precise recognition of complicated access behavior patterns (Equation 3).

$$r_s^{(j)} = e(V_{in}^{(j-1)} r_s^{(j-1)} + V_{rec}^{(j)} r_{s-1}^{(j)} + V_{cross}^{(j-1)} r_{s-1}^{(j-1)} + a^j) \quad (3)$$

Where the layer number is shown by superscripts and time steps are indicated by subscripts. Equation 3's V (j−1) cross hidden layer s−1 is the "cross" connection to create for hidden layers (j ≥ 2) from the lower layer in the preceding time step to improve information propagation.

### 3.2.3. Malleable Clouded – Leopard Optimization (MCLO)

The clouded leopard, a cat known for striking a balance between accessibility and caution, serves as the model for the optimization technique. The clouded leopard, which is neither enormous nor little, has a special combination of precision and flexibility. The MCL modeling approach is based on two distinct behaviors: the animal stays still during the day, surveying its environment from high vantage points, like tree canopies; at night, it deliberately descends to traverse intricate landscapes seeking food. The two stages of the MCL optimization process are reflected in these behavioral characteristics: adaptive ground interaction and strategic observation. By switching between exploration and exploitation, the model is able to fine-tune DRNN architectures for effective, instantaneous decision-making in situations involving dynamic cloud access administration. In Equations (4 and 5), the $n^{th}$ cloud leopard, $y_n^{o2}$, is the proposed new position.

$$y_{nm}^{o2} = y_{n,m} + \frac{p_m + rand_{n,m}.(v_m - p_m)}{s}.(2.rand_{n,m} - 1) \quad (4)$$

$$y_{n,m}^{o2} = IW_n(s) \cdot y_{n,m} + \frac{p_m + rand_{n,m}.(v_m - p_m)}{s}.(2.rand_{n,m} - 1) \quad (5)$$

An adaptive inertia weight (IW) mechanism is incorporated into the local search and exploitation phase to keep the optimization process from getting stuck in local optima. More responsive behavior is made possible during the optimization process by dynamically adjusting resources based on the cloud storage of this inertia weight according to each agent's current fitness. To encourage exploration, variety, and prevent premature convergence, IW is included in the MCL optimization phase. During the second step, also known as the capture phase, the adaptive IW directs the updating of the Clouded Leopard's positional vectors, improving the model's ability to identify globally optimum hyperparameters for in-the-moment access control choices.

The MCL method, which uses an adaptive operator $IW_n s$ (Equation (6)) to dynamically modify convergence behavior, is used to create an intelligent, self-optimizing access control framework for cloud computing. By integrating DL with a fitness-aware Versoria-based optimization mechanism, the framework improves real-time detection of anomalous access patterns. This guarantees scalable and accurate access control decisions in changing cloud environments, improves local search performance, and prevents premature convergence.

$$IW_n(s) = \begin{cases} 1 - \frac{1}{(\varphi.(b_m(s) - 1/2)^2 + 2)}, if\ b_n(s) \le 0.5, \\ \frac{1}{(\varphi.(b_n(s) - 1/2)^2 + 2)}, otherwisse, \end{cases} \quad (6)$$

To create a real-time cloud access control MCL system, PCA-based feature extraction and deep learning were used to improve security. By optimizing the model using clouded leopard ranking $P_n(s) \in [0,1]$, which reflects fitness between the mean and lowest, aberrant access patterns in dynamic contexts can be automatically detected in Equation (7).

$$P_{ave}(s) = \sum_{n=1}^{M_R} \frac{P_n(s)}{M_R}, \quad P_{min}(s) = \min\{P_1(s), P_2(s), \ldots, P_{M_R}(s)\}, \text{and} \quad (7)$$

$$b_n(s) = \frac{P_n(s) - P_{min}}{P_{ave}(s) - P_{min}} \quad (8)$$

Equation (8), the $P_{ave}(s)$ and $P_{min}(s)$ are the lowest and mean levels of the fitness of all $M_R$ size populations, respectively, and $P_n(s)$ is the fitness of the $n^{th}$ clouded leopard at iteration $s$. These parameters direct the DRNN model's optimization process, allowing adaptive learning to improve dynamic CC's real-time access control. Therefore, by reducing security risks while taking dynamic user behavior and environmental restrictions into account, the proposed optimization technique solves the issue of safe and effective access control in CC. As per the MCL method's presentation to improve the DRNN model, the framework selects the best access control decisions. Figure 3 displays MCL's systematic formulation and improvement plan.

The MCL-DRNN approach combines MCL optimization with DRNN to improve access control in dynamic cloud environments. DRNN temporal feature extraction to provide accurate classification with fiction. MCL improves learning by changing solution vectors according to clouded leopard-inspired adaptive

fitness-driven behavior. The approach reduces premature convergence and increases decision reliability by using adaptive inertia weights to balance exploration and exploitation.

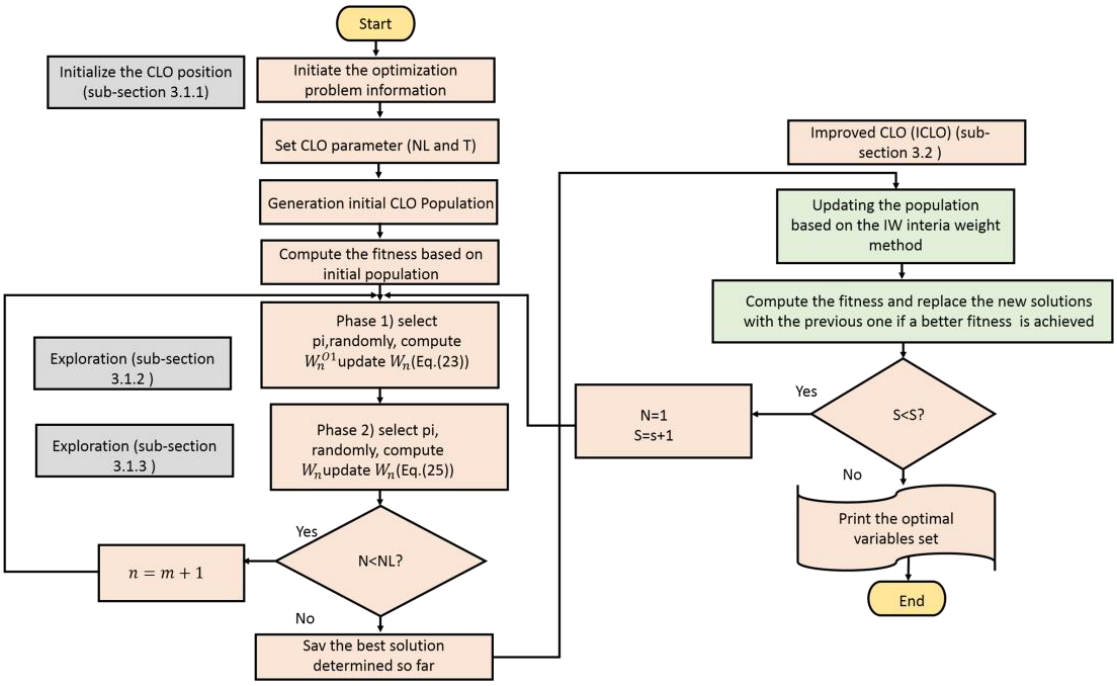


Figure 3. Flow chart for MCL

## 4. RESULTS AND DISCUSSION

In cloud environments, the MCL-DRNN method performs better than existing access control strategies when optimized using the MCL technique. Precision, recall, and F1-score are key performance measure that demonstrates exceptional ability to identify illegal access and adjust to changing user behavior. Using MCL in Python, the experimental setup optimizes DRNN hyperparameters for cloud access control. Utilizing an Intel Core i7 processor with 16 GB of RAM.

### 4.1. Feature Importance for Access Control Anomaly Detection

The real-time identification of anomalies using the MCL-DRNN model improves cloud security in Figure 4.

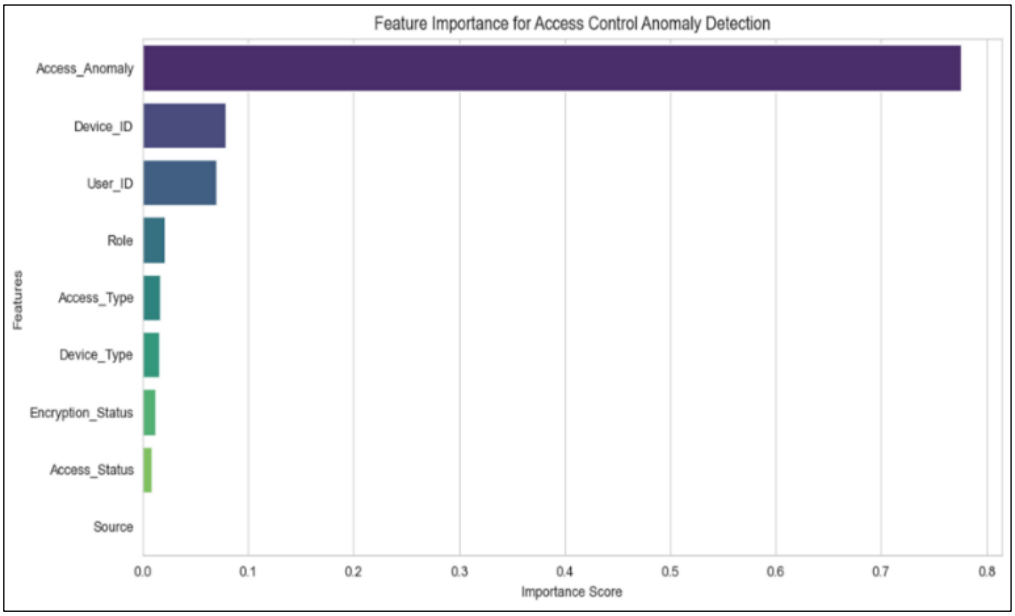


Figure 4. Correlation between different access control features in CC Environments

Tracking user activity and devices is crucial, and Access_Anomaly is the most important feature, followed by Device_ID and User_ID. Further enhancing access controls are Role, Access_Type, and Encryption_Status. By giving important aspects priority, MCL-DRNN responds to threats in real-time, assuring secure and intelligent cloud access.

### 4.2. Receiver Operating Characteristic (ROC)

The MCL-DRNN model's capacity to detect illegal access in a cloud environment is assessed using the ROC curve (Figure 5). Strong predictive skills are indicated by the high rise in the True Positive Rate (TRP) vs. False Positive Rate (FPR) plot. The model's capacity to distinguish between normal and anomalous access is demonstrated by near-perfect anomaly identification.

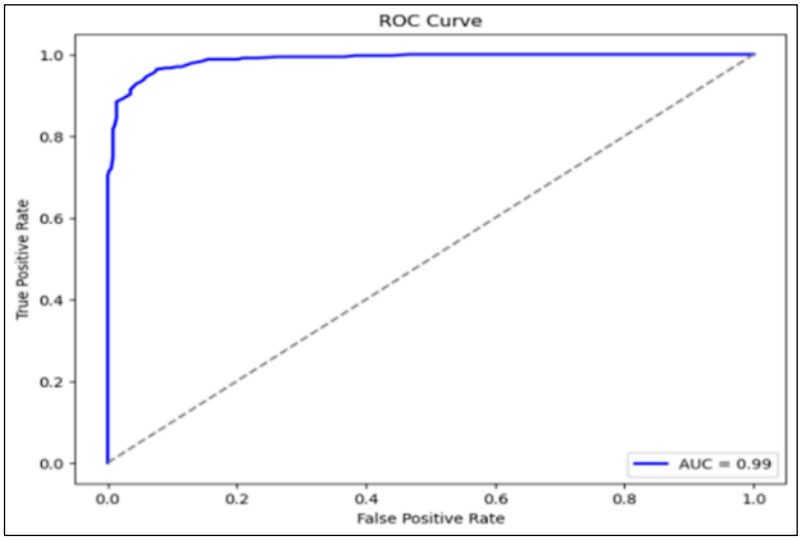


Figure 5. ROC Curve of MCL-DRNN

The proposed method, MCL-DRNN, was compared to Convolutional Neural Networks (CNNs) [20] and Artificial Neural Networks (ANNs) [20] using some metrics based on access control in a cloud environment.

### 4.3. Precision

Decreasing false positives in the access control system requires precision (Figure 6). By preventing legal users from involuntarily being classified as security threats, a high accuracy rating enhances user experience while maintaining security honesty. By differentiating between legitimate and suspect access requests, the MCL-DRNN form enhances precision, as shown in Equation (9).

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (9)$$

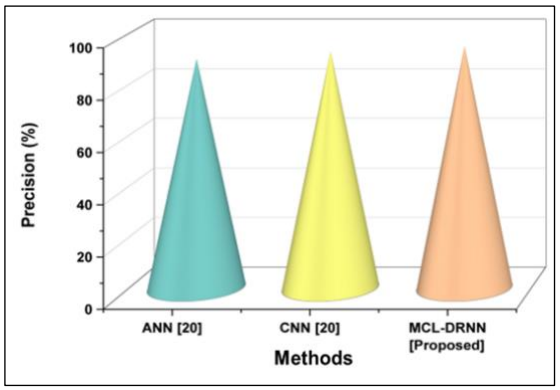


Figure 6. Evaluation metrics precision

### 4.4. Recall

Recall (Figure 7 (a)) plays a crucial role in the cloud system's ability to detect unwanted access attempts. Equation (10) can identify security vulnerabilities with a suitable recall score without ignoring important instances. To improve recall, the MCL-DRNN technique uses DL to detect compound access patterns and anomalies.

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \tag{10}$$

### 4.5. F1-score

The F1-score (Figure 7 (b)) provides a balanced measure of precision and recall, allowing the model to effectively remove both false negatives and false positives. As shown by Equation (11), the MCL-DRNN framework's robust F1-score demonstrates the ability to adapt to evolving cloud security risks while maintaining the precision of finding. Table 2 displays the numerical values for all metrics.

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{11}$$

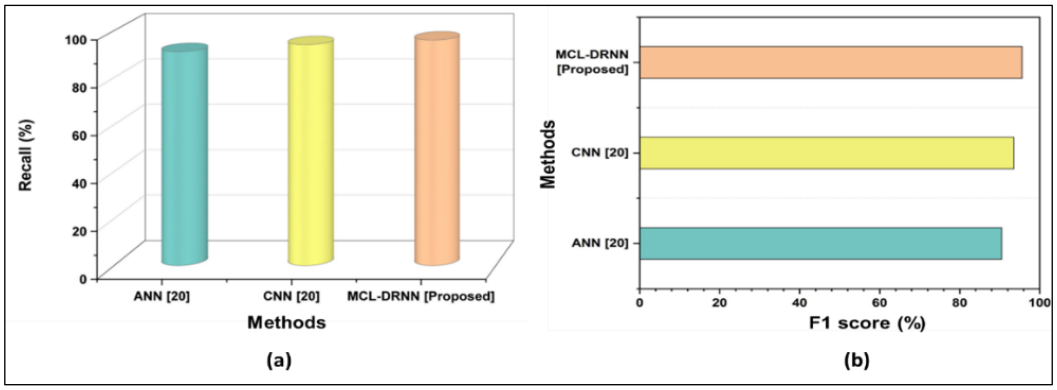


Figure 7. Outcome of metrics (a) recall, and (b) F1 score

Table 2. Comparison of existing and proposed methods

| Model | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|
| ANN [20] | 90 | 91 | 90.5 |
| CNN [20] | 93 | 94 | 93.5 |
| MCL-DRNN [Proposed] | 95 | 96 | 95.6 |

### 4.6. Missed Detection Rate (MDR)

MDR decreases the direct power on the system and security reliability, and greatly expands the function of the MCL-DRNN form in access control. Potential security breaches are avoided with a lower MDR, which precisely recognizes illicit access attempts. The mathematical formulation of MDR is expressed in Equation (12).

$$Missed\ Detection\ Rate = \frac{False\ Negative}{False\ Negative + True\ Positive} \tag{12}$$

### 4.7. False Alarm Rate (FAR)

The convenience of cloud services is further enhanced by lowering the FAR, which prevents official users from being mistakenly refused access. The FAR is stated in Equation (13). The MCL-DRNN method refines decision-making through continuous learning from cloud access logs, ensuring a balance between security and stability. Table 3 and Figure 8 show the rate metric for the proposed method.

$$False\ Alarm\ Rate = \frac{False\ Positive}{False\ Positive + True\ Negative} \tag{13}$$

Table 3. Impact of User Count on Missed Detection Rate and False Alarm Rate

| Number of Users | Missed Detection Rate | False Alarm Rate |
|---|---|---|
| 20 | 0.42 | 0.48 |
| 40 | 0.50 | 0.62 |
| 60 | 0.58 | 0.68 |
| 80 | 0.70 | 0.78 |
| 100 | 0.85 | 0.90 |

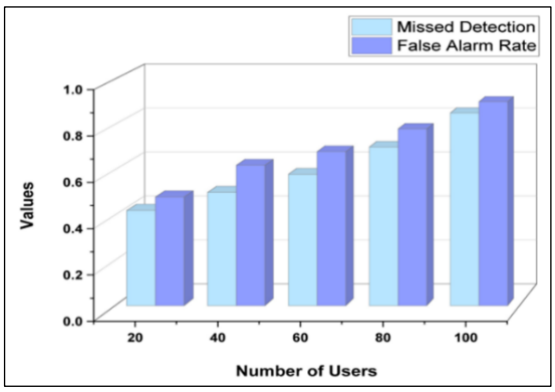


Figure 8. User-based metrics values for the proposed method

### 4.8. Discussion

In IoT-based healthcare systems, CNNs [20] and ANNs [20] present several challenges. CNNs are less appropriate for real-time applications in limited-resource situations because of high processing demands, reliance on huge labelled datasets, and poor interpretability. Dependability is further diminished by overfitting and vulnerability to hostile stimuli. Long preparation periods, scalability issues with deep frameworks, and the recurrent need for manual feature extraction are all issues with ANNs. When geographical data and noisy or incomplete inputs are present, performance tends to reduce. The challenges emphasize the need for DL techniques in healthcare to be more secure and efficient. For cloud access control, the MCL-DRNN framework has several benefits over traditional CNN and ANN models. Because of its recurrent nature, effectively ascertaining abnormalities in static models is regularly overlooked by capturing time-dependent user behaviour and access patterns. MCL-DRNN uses MCL tuning to enhance parameters in real-time, improving receptiveness to altering threats in contrast to ANNs and CNNs, which are less flexible. In addition, automated training was used to efficiently handle big, complicated datasets. For secure, real-time access control in dynamic cloud environments, MCL-DRNN is an intelligent, scalable, and self-optimizing solution.

## 5. CONCLUSION

For CC environments, the developed MCL-DRNN model offers intelligent, dynamic, and real-time access control solutions. The system proficiently captures complicated access behaviors and detects subtle anomalies by utilizing the sequential modeling capabilities of DRNNs with MCL tuning. An extensive dataset including IoT and CC healthcare access records was used for evaluation. The dataset demonstrated how well the algorithm integrated security systems, device operations, behavioral patterns and gesture-based activity data. The MCL-DRNN performs better than existing methods, based on performance comparisons, with an approximate 95% precision, 95.6% F1-Score and 96% recall. The framework has many drawbacks in spite of its excellent performance. The higher computational complexity cannot always be justified by small performance improvements over the existing methods. Furthermore, on devices with limited resources, the model can encounter challenges when dealing with sparse, noisy, or real-time streaming data. Future research will focus on expanding the training dataset for better generalization, simplifying the model for edge deployment, and improving interpretability for audit and compliance reasons.

## CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest in this work.

## DATA AVAILABILITY STATEMENT

The original data presented in the study are openly available at https://www.kaggle.com/datasets/programmer3/secure-access-control-dataset

## REFERENCES


[1] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT access control: Recent trends and future research directions," *J Netw Comput Appl*, vol. 203, p. 103371, Jul. 2022, doi: 10.1016/j.jnca.2022.103371.

[2] M. Mehrtak *et al.*, "Security challenges and solutions using healthcare cloud computing," *J Med Life*, vol. 14, no. 4, pp. 448–461, Aug. 2021, doi: 10.25122/jml-2021-0100.

[3] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digit Commun Networks*, vol. 9, no. 2, pp. 411–421, Apr. 2023, doi: 10.1016/j.dcan.2022.11.003.

[4] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey," *Cluster Comput*, vol. 28, no. 8, p. 529, Sep. 2025, doi: 10.1007/s10586-025-05308-x.

[5] S. El Kafhali, I. El Mir, and M. Hanini, "Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing," *Arch Comput Methods Eng*, vol. 29, no. 1, pp. 223–246, Jan. 2022, doi: 10.1007/s11831-021-09573-y.

[6] A. A. Abd-Aljabbar, D. A. Hammood, and L. H. Abed, "Secure Cloud Storage Using Multimodal Biometric Cryptosystem: A Deep Learning-Based Key Binding Approach," *J Al-Qadisiyah Comput Sci Math*, vol. 17, no. 1, Mar. 2025, doi: 10.29304/jqcsm.2025.17.11976.

[7] R. S. K. Boddu *et al.*, "Using deep learning to address the security issue in intelligent transportation systems," *J Auton Intell*, vol. 7, no. 4, Mar. 2024, doi: 10.32629/jai.v7i4.1220.

[8] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," *Int J Eng Bus Manag*, vol. 14, Nov. 2022, doi: 10.1177/18479790221093992.

[9] M. Tahir, M. Sardaraz, Z. Mehmood, and S. Muhammad, "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security," *Cluster Comput*, vol. 24, no. 2, pp. 739–752, Jun. 2021, doi: 10.1007/s10586-020-03157-4.

[10] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by Design for Big Data Frameworks Over Cloud Computing," *IEEE Trans Eng Manag*, vol. 69, no. 6, pp. 3676–3693, Dec. 2022, doi: 10.1109/TEM.2020.3045661.

[11] V. K. Ravi and A. Ayyagari, "Data Lake Implementation in Enterprise Environments," *SSRN Electron J*, 2025, doi: 10.2139/ssrn.5068537.

[12] K. R. Bellala, "AI Driven Zero Trust Security for Hybrid Clouds," *Int J Innov Sci Res Technol*, pp. 1492–1497, Apr. 2025, doi: 10.38124/ijisrt/25apr1143.

[13] A. Singhal, P. Kumar Goel, D. Garg, and C. Sharma, "Enhancing Cloud Performance with AI-Driven Load Balancing and Optimization Algorithms," in *2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE)*, IEEE, Nov. 2024, pp. 1254–1259. doi: 10.1109/AECE62803.2024.10911072.

[14] Bukunmi Temiloluwa Ofili, "Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience," *Int J Comput Appl Technol Res*, Mar. 2025, doi: 10.7753/IJCATR1209.1003.

[15] M. Sadaf *et al.*, "Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects," *Technologies*, vol. 11, no. 5, p. 117, Sep. 2023, doi: 10.3390/technologies11050117.

[16] U. S. Basha, "Fortifying Healthcare Data Security in the Cloud: A Comprehensive Examination of the EPM-KEA Encryption Protocol," *Comput Mater Contin*, vol. 79, no. 2, pp. 3397–3416, 2024, doi: 10.32604/cmc.2024.046265.

[17] A. F. Mammo *et al.*, "Multimodal Bio Cryptography for Securing Cloud Computing using Convolutional Neural Network," in *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/IC3TES62412.2024.10877575.

[18] N. Mohammadi, A. Rezakhani, S. H. H. Seydjavadi, and P. Asghari, "Enhancing Time-Series Access Control Using Deep Recurrent Neural Networks and Generative Adversarial Networks," August 22, 2024. doi: 10.21203/rs.3.rs-4791025/v1.

[19] M. Alanazi, A. Alanazi, K. M. AboRas, and Y. Y. Ghadi, "Multiobjective and Coordinated Reconfiguration and Allocation of Photovoltaic Energy Resources in Distribution Networks Using Improved Clouded Leopard Optimisation Algorithm," *Int J Energy Res*, vol. 2024, no. 1, Jan. 2024, doi: 10.1155/2024/7792658.

[20] K. Thilagam *et al.*, "Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System," *J Nanomater*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/2638613.

**BIOGRAPHIES OF AUTHORS**

**Aditya Gupta** is working as a Research Associate in Computer Science and Engineering at Lincoln University College, Malaysia and also working as a Senior Software Developer in a reputed organization in Lucknow, UP, India. He can be contacted at email: gupta.aditya56@gmail.com

**Sai Kiran Oruganti** is a professor specializing in wireless power transfer and IoT security, currently affiliated with Jiangxi University of Science and Technology in China and Lincoln University College in Malaysia. His career includes research at the Ulsan National Institute of Science and Technology, developing wireless systems for Hyundai and Samsung, a faculty position at the Indian Institute of Technology, and a recognized history of innovation, including pioneering work on Zenneck Wave WPT and over 16 granted patents. He can be contacted at email: saisharma@lincoln.edu.my