International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I6P102

Volume 74 Issue 6, 17-32, June 2026

Original Article

Behavioral Authorization Framework for Cloud Environments using Deep Representation Learning and Discriminative Decision Modeling

Mandeep Kaur[1], Prachi Garg[2]

[1]*CSED, Maharishi Markandeshwar University (Deemed to be University), Ambala Assistant Professor, PIET, Samalkha, Panipat, Haryana, India.*
[2]*CSED, Maharishi Markandeshwar University (Deemed to be University), Ambala, Haryana, India.*

[1]*Corresponding Author : mandeep.kaur79@gmail.com*

Received: 30 June 2025 Revised: 07 April 2026 Accepted: 20 April 2026 Published: 27 June 2026

Abstract *- The security of any system is as good as the authentication mechanism used to access it. Authentication verifies user identities in systems such as cloud applications, services, or data. Traditional passwords, Identity and Access Management (IAM), OTPs, and Multi-Factor Authentication (MFA) are increasingly vulnerable to cyber threats, including identity theft, account hijacking, and spoofing attacks due to advancements in AI, improvements in hardware, and inexpensive computational power. Considering these challenges, there is a need to develop mechanisms that do not rely solely on simple authentication techniques but are robust and continuous. Researchers are also focusing on developing the use of keystroke dynamics for authentication and developing AI and machine learning models for security. This work proposes a novel behavioral authentication framework based on a hybrid CNN_SVM model for continuous user verification, which secures against unauthorized access and breaches in Cloud environments. It considers various behavioral biometrics, including keystroke dynamics, touch patterns, pressure points, mouse movement patterns, touchpad pointer, device properties, time of use (when), usage pattern (how and frequency), and user interaction with the interface for real-time continuous user authentication. First, a comprehensive dataset of user behavior traits is collected, then preprocessed for feature normalization, and finally, dimensionality reduction and feature engineering are applied. It uses CNN to learn high-level behavioral patterns in the dataset, and an SVM classifier to optimize discrimination between legitimate users based on their activities. It evaluates and compares the use of SVM_CNN, RESNET_SVM, Random Forest, XGBoost, and Decision Tree machine learning models in validating the effectiveness of the proposed framework. The results show that the SVM_CNN model yields the best accuracy of 0.85, precision of 0.8658, recall of 0.8789, F1 score of 0.8723, and ROC AUC of 0.8855 compared to the existing approaches. The ablation study compares the criticality of different model components: data augmentation, pre-trained weights, batch normalization, and dropout regularization in classification accuracy. Moreover, the feature count analysis shows an accuracy gain of up to 0.85 when the behavioral features increased from 2 to 12. Experimental results confirm that the proposed hybrid CNN_SVM behavioral authentication system provides a robust, scalable, and intelligent solution. It achieved better performance due to the addition of reading, typing, time, and device-related features rather than only using typing-related features for authentication. It can be used as a continuous, frictionless, and adaptive authentication mechanism for cloud security by integrating it with their traditional mechanisms. If integrated accordingly, it shall ensure the detection of security anomalies and take proactive actions to strengthen the security, while supporting other regulatory compliance.*

Keywords *- Authentication, Behavioral Authentication, Cloud Computing, Machine Learning, Security.*

1. Introduction

Cloud authentication is the process of verifying claimed identities across the cloud platform. It confirms whether the user is the one he claims to be. It is the first line of defence that verifies user identity before allowing access to cloud services, including platforms, infrastructure, and other resources, based on their access rights and privileges. Strong, effective cloud authentication techniques are important for safeguarding against a range of threats and attacks. However, attacks such as disclosure of sensitive information, Denial-Of-Service (DoS), spoofing, data tampering, repudiation, hijacking of accounts, and privilege elevation are common threats to Cloud security [1, 2], including network layer attacks like DoS, Man-in-the-Middle (MITM), and Replay attacks. Application-layer attacks such as Known Session-specific Temporary Information (KSSTI), malware injection,

and customer fraud are also prominent. Other attacks, like Password Discovery attacks, Reflection attacks, and Insider attacks [3], are also possible on cloud platforms. It is evident that different authentication techniques may restrict many such attacks. Password-based methods are simple yet vulnerable to brute-force, phishing, and reuse attacks. Token-based mechanisms like OTPs and session tokens reduce replay attacks but rely on alternate devices that may be compromised. Alternatively, organizations are looking forward to behavior-based authentication to enhance security, productivity, reduce the risks associated with compromised passwords, address compliance regulations, and promote enterprise mobility. Among the latest mechanisms, behavioral authentication or behavioral identity authentication is most promising [4] due to its properties of being frictionless, continuous, synthesizable, and inherent [5, 6]. It is evolving due to advancements in artificial intelligence and improvements in hardware, thereby increasing dependence on types of devices used to access cloud services. Initially, collected behavioral data has been used for target authentication scenarios with usability requirements [7, 8]. Behavioral identity authentication guards against both external attackers and malicious insiders who have access to a Cloud's physical or digital assets. Over time, researchers are digging deeper into exploring the scope of applications for behavioral authentication mechanisms, focusing on their robustness, reliability, and timeliness to ensure overall security and protection.

1.1. Behavioral Authentication

Behavioral authentication is a cutting-edge technology revolutionizing the security aspects of computing. It is based on the composite pattern(s) of interactive behavior of individuals that can be associated with users to uniquely identify them as they interact with devices, systems, and applications [9]. According to a study by Forrester Research, the use of behavioral biometrics can reduce the false positives in fraud detection by half [10]. It can also identify individuals without the need for using traditional forms of authentication, such as passwords or tokens. This is possible as each person has a unique set of behaviors that can be used to identify them on the go.

1.1.1. Behavioral Authentication Studies

Behavioral identity authentication uses the behavior of individuals' interactions with their computers to authenticate users, which is as unique as fingerprints [11] and provides a more secure experience to the users. It is passive [12, 13] since it does not require a specific user action for authentication [14]. It is categorized into five major types: keystroke dynamics, touch gestures, gait, motion-based analysis, intrinsic signaling, and behavioral patterns in user interaction.

- Keystroke-based authentication verifies the user's identity by analyzing the speed, typographic speed, errors, and other characteristics on the keyboard.
- Touch gesture-based authentication methods complement the shortcomings of keystroke-based methods by analyzing interaction behavior collected using gestures or touches.
- Motion-based authentication considers user motion data like gait, limb movement, speed variations, and orientation collected through various sensors like wearable and mobile devices having accelerometers and gyroscopes, for the authentication of individuals.
- Intrinsic signals are generated by body parts that can be used for authentication. Some researchers worked on the use of EEG records (electrical activity of the brain), EMG records (electrical activity of muscles), both at rest and during contraction, and ECG (electrical activity of the heart) in authentication using their rhythm and rate. Exploration is underway into the use of breath, facial expressions, and voice patterns, which are highly unique and hard for attackers to replicate.
- User interaction behavior, such as search history, transactions, user profile, sensitivity, and other devices used during interaction in some specific way, can also be used for identification.

2. Literature Review

Initially, behavioral authentication is an emerging domain in cloud security that focuses on the validation of user identities using the patterns of users' behavior. Work on this strategy is fairly recent, paying attention to many of its facets, its potential, and its limitations. As indicated in [4], a robust behavioral model of applying composite behavioral records generated from online social networks was utilized for detecting online identity theft.

These models are synthesizable both in terms of how users behave online and offline. Its AUC of 0.956 in the public dataset of Foursquare and 0.947 in Yelp is better than other existing models. In general, when the disturbance rate is below 1%, the recall can reach up to 65.3% in Foursquare and 72.2% in Yelp with low response latency. Finally, this work sheds new light on how to improve the real-time online identity authentication based on the modeling of the users' composite behavioral patterns.

In [13], Shakir reviews existing research work on authentication methods used in public clouds concerning behavior authentication. It highlights that the existing Multifactor authentication technologies, smart card passwords, mobile, and biometrics, are vulnerable to stolen password attacks [14].

Finally, the paper suggests that intelligent authentication operations can provide the best way to improve authentication accuracy in the public cloud computing environment. Most popular suggested models include [15], in which Mostafa et al. propose "an adaptive multi-factor multi-layer authentication scheme" to improve the security of a cloud

platform with low false positive alarms. It presents an automated authentication method selection with access control and intrusion detection mechanisms. To strengthen identity verification, multiple authentication factors such as user factors, geolocation, and browser confirmation are implemented on the system. On top of that, AES-based encryption is used to avoid the disclosure of data. The framework claims to identify malicious users and intruders and prevent any intentional attacks on the services as well as the data of cloud servers.

In [16], Olabanji et al. compare AI-driven user behavioral authentication with the traditional security measures in the cloud environment. It shows that both methods lead to improved threat detection accuracy compared to the traditional methods. Systems driven by such an AI-driven approach [17] offer better predictive capabilities and performance in terms of security. An alternative approach would be to combine 'hybrid security', considering a hybrid security strategy to deal with cloud-related cyber threats. According to Carmel & Akila [18], an exhaustive survey has been given on biometric solutions to resolve cloud security issues related to Identity theft.

Earlier, many protocols involving biometric authentication had been proposed for the cloud environment to combat Identity theft [19]. Based on a similar approach, Alsirhani et al. presented an advanced IAM framework for managing the entire lifecycle of user identities and entitlements across different enterprise resources in public and private cloud platforms [20-22].

As an improvement to the data security of the cloud environment, Fathima & Saravanan [23] proposed a Multifactor Authentication (MFA) framework, something the users know, have, or are [24], on the weakly human-controlled factors. The three phases included in this framework are user registration, login, and continuous authentication.

To come up with a unique 6-digit PIN, users supply a lot of data to register. Static, dynamic, and possession are the factors that are used for authentication at the time of login. The user's typing behaviour is used to calculate trust scores. Secure PINs are used for critical operations, while re-authentication requests are made when needed. The proposed model surpassed all by their performance, with 99.4% robustness, 99.7% accuracy, and 0.3% error rate in both the closed and the open datasets.

It greatly improves security in cloud systems to the benefit of end users and cloud service providers. Kumar and Ray [25] suggest an authentication model that analyses the applicant's usage patterns employing machine learning techniques to detect unusual user behavior. The designed data mining model is used for developing a behavior-based authentication system for mobile devices, applying PSO for feature selection and C4.5 and J48 decision trees for learning and classification on a keystroke dataset, achieving 90.01% classification accuracy [26, 27].

In [28], Reddy et al. performed a study where each user typed the 11-character text "Exponential" 8 times. The key press and release times were recorded for all 90 users. It aimed to test whether keystroke dynamics can be used for user authentication. The dataset was compartmentalized into tiers such as key press time, durations, latencies, and digraphs. Using these features, Decision Tree, Multi-layer Perceptron, and LightGBM were applied for evaluation. It was found that the use of multiple-tier features significantly improved the models, leading to better results.

The use of more granular patterns and relationships in keystroke data resulted in better results. In [29], El-El-Sofany presented a Cloud-Based Biometric Authentication Model (CBioAM) that claims to increase the security of cloud services. The model uses the biometric samples pre-stored in the database servers and performs the authentication process without requiring much of the user's information for the evaluation of accuracy, sensitivity, and specificity.

The implementation of the model is done using a novel algorithm called 'Bio_Authen_as_a_Service'. Experimental results show a performance average of 93.94% and an accuracy average of 96.15%. Rao et al. in their work [30] discussed the use of a behavioral analysis approach for preventing insider attacks in the Cloud environment.

The behavioral features can act as a security solution as proposed in [31]. Researchers explored various authentication techniques in computing comprehensively, including traditional methods like articles, letters, passwords, digital certificates, two-way authentication techniques, behavioral profiles, doodles, image sequences, biometrics, gait, and behavioral analytics, discussing their key features and potential for further improvement, like encryption of the biometric information of users and farmed out for the Cloud database in an encrypted server [32].

A novel multimodal biometric authentication scheme based on feature fusion [33] has also been proposed. Sajad et al. described how a deep learning approach can be used for face spoofing detection systems in an IoT cloud-based environment [34] that was tackled using multimodal biometric systems [35].

It explored the use of fast feature selection based on Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO) for feature extraction and classification process [36] that uses the integration of face and fingerprint texture patterns to identify individuals.

Table 1. Comparison of some behavior-based authentication models

Paper	Method used	Based on	Dataset Used	Limitation(s) / Research Gaps
[37]	Keystroke dynamic-based recognition system	probability distributions of the typing times for each typist	Self-populated dataset of features of 4 typists	Provided the idea of using keystroke statistics
[38]	Multi-Layer Perceptron	Used Error Rate (EER), Accuracy, Precision, Recall, and ROC curve to evaluate performance	CMU dataset (sample size=51) under a controlled environment	AUC not used
[39]	CNN, Transformers, LSTM	Hold-out and classification approach	Publicly available dataset (sample size=13)	Trained models cannot accurately classify new samples
[40]	GA-KNN	KNN is used to classify users as genuine and impostors	GREYC dataset (sample size=100) in a controlled environment	High intra-class variability in the keystroke and mouse behavior. User behavior evolves over a period of time then model performance is changed.
[41]	Convolutional Neural Network	Used a 5-character length code for each user for comparison	CMU dataset (sample size=51) under a controlled environment	Trained models cannot accurately classify new samples
[42]	Convolutional Neural Network	Used feature extraction from the raw behavioral data of users	The dataset (sample size=150 in a semi-controlled environment	Adaptive mechanism, AUC, FAR, FRR, RMSE, Precision, F-measure not used
[43]	RF, KNN, GBC, followed by TypeNet and TypeFormer transformers	Used EER to evaluate the authenticity of the user	The Palin dataset, with a sample size of 31400, is in an uncontrolled environment.	Adaptive mechanism, AUC FAR, FRR, Accuracy, RMSE, Precision, F-measure, not used in keystroke behavioral biometric
[44]	STDAT-based BehaveFormer	Performance comparison of behavior-based authentication with different datasets	HMOGdb with sample size=99, HuMIdb dataset with sample size=428, Palin and PETA datasets were compared.	Adaptive mechanism, AUC, FAR, FRR, Accuracy, RMSE, not used in behavioral biometrics
[45]	RNN-TypeNet Architecture	Keystroke-based biometric authentication involving a large amount of text	Dhakal dataset with sample size=168000 and an uncontrolled environment	Adaptive mechanism, AUC, FAR, FRR, Accuracy, RMSE, not used in keystroke behavioral biometric
[46]	Transformer	Keystroke-based data was used	The Palin dataset, with a sample size of 30400, is in an uncontrolled environment.	Adaptive mechanism, Precision, F-measure not used in keystroke behavioral biometric

3. Research Problem and Novelty

The paper presents the use of multiple behavioral parameters in authentication using the proposed SVM-CNN-based approach. To design and implement a behavioral authorization framework for Cloud environments that uses typing, reading, comprehension, solving, typographical errors, speed, accuracy, device types, time of access, mouse/touchpad behavior over laptops/desktops, and re-validate the users by classifying them as legitimate or fake ones using deep learning and discriminative decision modeling. It collected a novel dataset of users in a controlled environment during the registration process. Then, it uses this data for runtime classification of users. If the legitimate user verifies the use during drift in behavior, the data gets updated by adding records as ‘legitimate user’ in the dataset or adding a new row classified as ‘fake user’ with that set of details. The design is novel and original in considering patterns in time of day of access, choice of device(s), and changes in patterns, reading behavior, retention, and cognitive properties like answerSpeed, readingSpeed, and user engagement, also for making a behavioral profile. It adds to the currently suggested models that use typing or touch-related behavior analysis for authentication, rather than the already available models. Further sections detail the proposed methodology, experimental results, and analysis, including comparison with other available methods, and an ablation test of the features used. Finally, the conclusive remarks have been placed for ready reference.

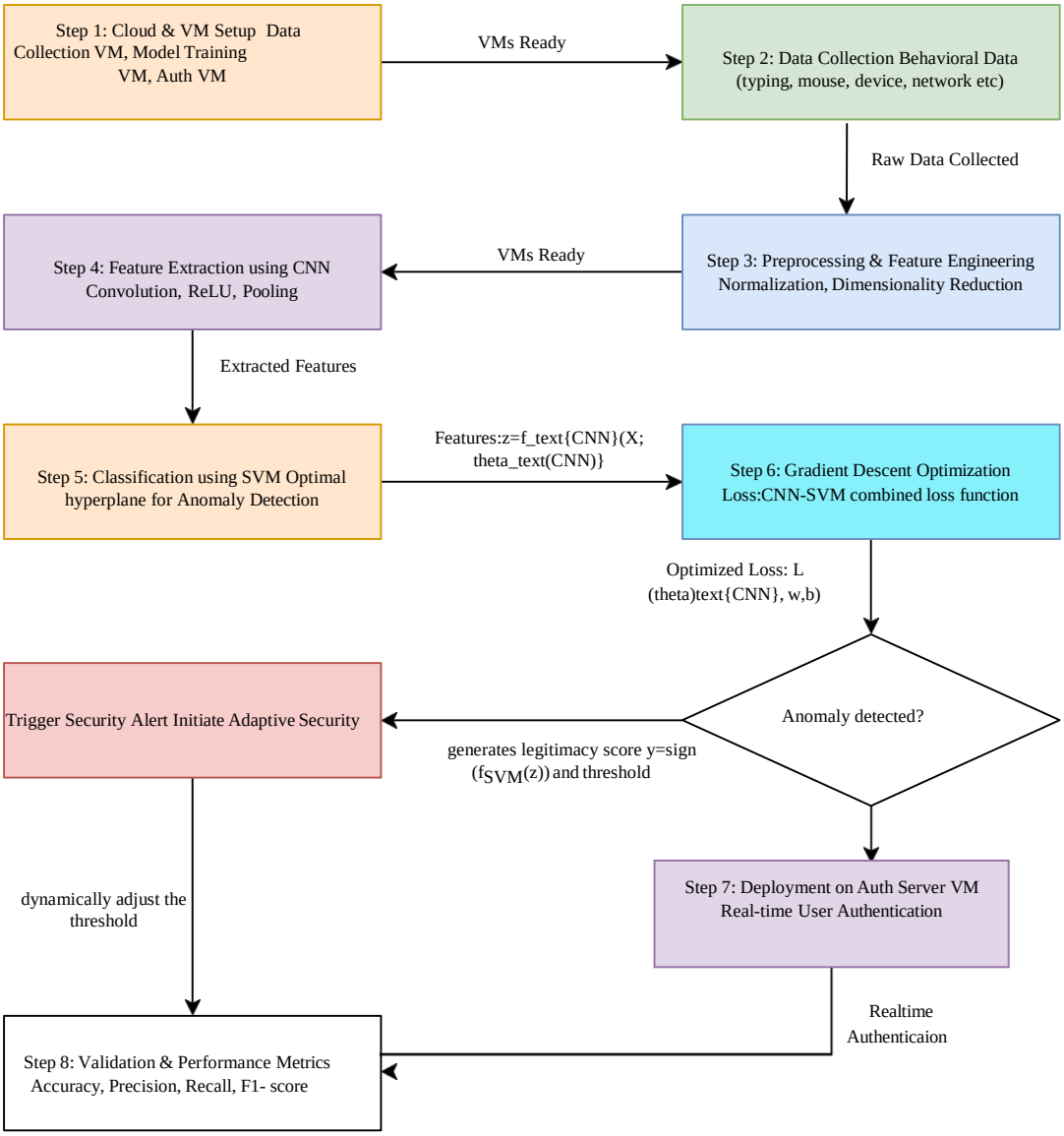

Fig. 1 The proposed 8-step methodology

4. Proposed Methodology

The eight-step proposed methodology (as shown in Figure 1) is used to provide the proposed SVM-CNN-based approach for the design of a behavioral authorization framework using deep representation learning and discriminative decision modelling.

4.1. Step 1: Cloud and Virtual Machine Setup

4.1.1. Setting Up Cloud Infrastructure

To deploy your machine learning models and authentication mechanisms, you need a cloud environment where you can run VMs and allocate resources as needed. The steps are:

- Data center Setup: In your cloud environment, create a data center that consists of physical resources such as CPUs, memory, and storage.
- VM Creation: Launch Virtual Machines (VMs) for different purposes, such as:
  a) Data Collection VM: For gathering and preprocessing the behavioral data (typing patterns, mouse movements, network activity).
  b) Model Training VM: For training and running your hybrid CNN-SVM model.
  c) Authentication Server VM: For deploying the authentication mechanism and verifying users in real-time.

VMs are then created and configured on a private cloud infrastructure platform, OpenStack, since it is free to use. The same can be done on other platforms: VMware ESXi or Proxmox, as per the choice or availability.

4.1.2. Setting Up Cloud Infrastructure

Each VM is equipped with the following resources for the tasks:

- Data Collection VM: Moderate resources for handling user session data and behavior analysis.
- Model Training VM: High computing resources (e.g., GPUs or CPUs) for running the CNN-SVM model training.
- Authentication Server VM: Moderate computing power to continuously authenticate users.

4.2. Step 2: Cloud and Virtual Machine Setup

Behavioral data is collected continuously from users interacting with the system. This data is processed on the Data Collection VM and then stored in a distributed file system or a centralized data store for future processing.

4.2.1. Data Sources

- Typing patterns: Collect data such as typing speed, keystroke dynamics for each character, frequently erroneously typed words, max./min. Speed, time for switching from a lower letter to a capital letter, use of numeric keys, special keys, unnecessary pressing of the refresh button, and time intervals between keystrokes.
- Mouse movement patterns: Track mouse movements like velocity, click patterns-multiple clicks instead of single ones, use of mouse refresh options, use of path trajectory.
- System and Network characteristics: Monitor latency, using multiple applications during work, switching programs, application usage, packet loss, machine details, and source IP addresses to detect abnormal network behavior.

Data is transmitted from the user's local machine to the Data Collection VM via a secure channel (e.g., using SSL/TLS).

4.3. Step 3: Preprocessing and Feature Engineering

On the Data Collection VM, the raw behavioral data is preprocessed to remove noise, normalize values, and convert the data into a format compatible with the machine learning model.

- Normalization: Scale the values of features like typing speed and mouse movement velocity to a standard range.
- Dimensionality Reduction: Apply Principal Component Analysis (PCA) to reduce the feature space for more efficient training.

The preprocessed data is stored for training on the Model Training VM.

4.4. Step 4: Feature Extraction using CNN on VM

The Model Training VM is responsible for training the Convolutional Neural Network (CNN) for feature extraction.

4.4.1. CNN Training Process

- The preprocessed data is loaded into the VM.
- The input behavioral data (e.g., mouse and typing patterns over time) is structured into matrices $X \in \mathbb{R}^{m \times n}$ where m represents the number of features (typing speed, mouse velocity, etc.) and n represents the time steps or instances collected.

4.4.2. CNN Architecture:

- Input Layer: The input data is passed into the CNN.
- Convolutional Layers: Apply filters to extract high-level behavioral patterns.
- ReLU Activation: Introduce non-linearity using ReLU activation.
- Pooling Layer: Apply pooling to reduce the spatial dimensions of the dataset of the feature map.
- Fully Connected Layer: The flattened feature map is passed through fully connected layers to generate a feature vector.

The output from the CNN is shown in Equation (1),

$$z = f_{\text{CNN}}(X; \theta_{\text{CNN}}) \tag{1}$$

represents the learned features.

4.5. Step 5: Classification Using SVM on VM

Once the CNN extracts the features from the behavioral data, an SVM is trained to classify whether a user's session is legitimate or anomalous.

4.5.1. SVM Model Setup on VM:

- Feature Input: Use the output feature vector z from the CNN.
- SVM Objective: The SVM finds the optimal hyperplane to classify the behavior in Equation (2):

$$f_{\text{SVM}}(z) = w^T z + b \tag{2}$$

Where w is the weight vector, and b is the bias term.

- SVM Optimization: The SVM solves the following objective function in Equation (3):

$$\min_{w,b} \frac{1}{2} \| w \|^2 + C \sum_{i=1}^{m} \max\left(0, 1 - y_i(w^T z_i + b)\right) \tag{3}$$

- The SVM is trained on the Model Training VM using gradient descent optimization for the CNN parameters. θ_{CNN} and the SVM parameters w and b.

4.6. Step 6: Gradient Descent Optimization on VM

Gradient Descent is used to optimize the parameters of both the CNN and the SVM algorithms:

4.6.1. Loss Function for Hybrid CNN-SVM

- The total loss function combines both the CNN feature extraction loss and the SVM classification loss as presented in Equation (4):

$$L(\theta_{\text{CNN}}, w, b) = \frac{1}{2} \| w \|^2 + C \sum_{i=1}^{m} \max\left(0, 1 - y_i(w^T f_{\text{CNN}}(X_i; \theta_{\text{CNN}}) + b)\right) \quad (4)$$

Gradient Updates: The parameters are updated using gradient descent in different ways, as mentioned in Equations (5) to (7):

- CNN Parameters Update is provided in Equation (5):

$$\theta_{\text{CNN}} \leftarrow \theta_{\text{CNN}} - \eta \frac{\partial L}{\partial \theta_{\text{CNN}}} \quad (5)$$

- SVM Weights Update is done w.r.t. Equation (6):

$$w \leftarrow w - \eta \frac{\partial L}{\partial w} \quad (6)$$

- SVM Bias Update is done as per Equation (7):

$$b \leftarrow b - \eta \frac{\partial L}{\partial b} \quad (7)$$

Where η is the learning rate.

This training and optimization process runs on the Model Training VM.

4.7. Step 7: Deployment of Real-Time Authentication on the Authentication Server VM

Once the model is trained and optimized, the final step is to deploy it on the Authentication Server VM.

It is responsible for real-time, continuous authentication of users by analyzing the collected data using the trained model.

4.7.1. Real-Time User Authentication

The behavioral data from a user's current session is collected and passed through the trained CNN-SVM model deployed on the Authentication Server VM. The model generates a legitimacy score, and the decision function $y = \text{sign}\left(f_{\text{SVM}}(z)\right)$ determines whether the session is legitimate or anomalous.

4.7.2. Adaptive Security

The system can dynamically adjust the threshold τ for anomaly detection based on the sensitivity of the data being accessed or the behavior context (e.g., location, time of day).

4.8. Step 8: Validation and Performance Metrics

The system's performance metrics of accuracy, precision, recall, F1-score, and AUC-ROC are evaluated for the model. These are useful in examining whether the suggested model will be useful for the authentication of users based on the proposed criteria or not.

- Accuracy: measures the overall correctness of the predictions.
- Precision: shows the proportion of legitimate behaviors identified correctly.
- Recall: measures how many legitimate sessions are correctly classified.
- F1-Score: measures the balance between precision and recall.
- AUC-ROC: calculates the system's ability to distinguish between legitimate and anomalous behavior.

5. Results and Discussion

5.1. Feature Analysis

The correlation heatmap of typing features is shown in Figure. 2, which shows the relationships among different typing characteristics.

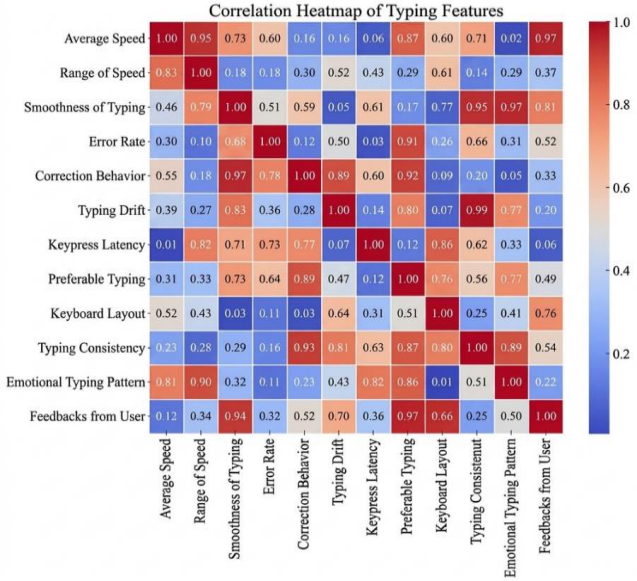

Fig. 2 Feature information by correlation

The higher the correlation value (shown in red), the stronger the relationship; the lower the correlation value (marked in blue), the weaker the relationship.

5.1.1. Statistical Analysis

The heatmap reveals that 'Average Speed' and 'Feedback from Users' have a strong positive correlation (0.97), which means that the users who type faster get better feedback. Similarly, 'Preferable Typing' and 'Smoothness of Typing' have appreciably high Pearson correlation of 0.95, signifying that the users who have smoother typing patterns have a more preferable typing style. 'Error rate' also has a strong correlation (0.92) with 'Correction Behavior', as could be expected, as those who make more corrections are likely to have a higher error rate.

Curiously, 'Keypress Latency' has almost zero correlation (0.01) with 'Average Speed', and 'press time' does not notably contribute to the overall speed. Although 'Preferable Typing' is strongly correlated (0.86) with 'Keypress Latency', it suggests that users who prefer their typing style tend to have more consistent keypress timings.

Also, there is a relatively high correlation (0.90) between 'Emotional Typing Pattern' and 'Average Speed', suggesting users' emotions can significantly affect the typing speed. On the other hand, a few features that have weak correlations with most of the other attributes. For example, 'Keyboard Layout' has correlations of less than 0.27 with all attributes except Preferable Typing (0.76). The implication is that 'layout preference' in the choice of keyboards used by users does not affect their 'speed' and 'accuracy', but relates well to overall comfort.

5.1.2. Implications

This overall heatmap provides valuable insights into how different factors of typing behavior are related to each other and which user typing patterns may be used for authentication.

5.2. Performance Metrics

Different machine learning models were used to classify users as 'genuine' or 'not genuine' based on behavioral data for authentication. RSENET-based models - RESNET_SVM, RESNET_RandomForest, RESNET_XGBoost, RESNET_DecisionTree were used for classification, and their performance metrics were compared. The data related to Accuracy, Precision, Recall, F1Score, and ROC_AUC are presented in Table 1, and the bar chart for visual comparison is provided in Figure 3. Based on the statistics, the following descriptive statistical analysis can be drawn:

Table 2. Proposed model comparison with existing approaches

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RESNET_SVM	0.85	0.861237	0.825745	0.843118	0.896903
RESNET_Random Forest	0.84	0.844108	0.831824	0.837921	0.880262
RESNET_XGBoost	0.85	0.835442	0.861611	0.848324	0.861588
RESNET_Decision Tree	0.63	0.650364	0.62689	0.638412	0.665468

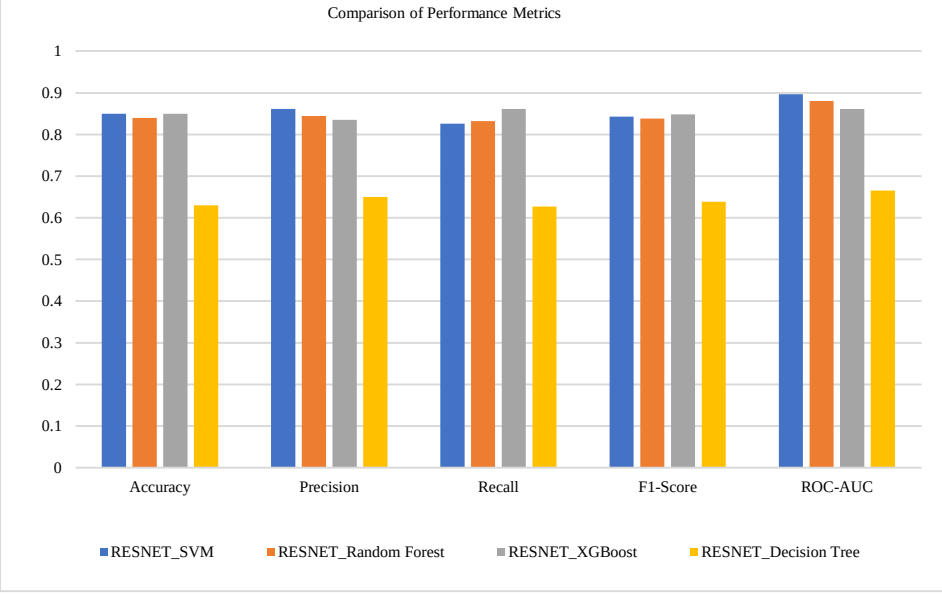

Fig. 3 Comparison of performance metrics

5.2.1. Comparative Performance Analysis

Accuracy

The models RESNET_SVM and RESNET_XGBoost achieve the highest accuracy of 0.85, the highest among all models, and provide superior, consistent performance. These can correctly classify the majority of the instances. However, RESNET_DecisionTree provides poor classification capability.

Precision

RESNET_SVM yields the best precision (0.8612) and is more reliable for positive instance prediction with the lowest false-positive rate among all options.

It shall perform better in high-security applications, such as user authentication.

Recall

RESNET_XGBoost has the highest recall (0.8616), signifying it is better at identifying actual positive instances with minimal false rejections.

F1-Score

The gap between the F1 scores of the two models – RESNET_SVM (0.8431) and RESNET_XGBoost (0.8483) is very small, thereby indicating a balanced trade-off between precision and recall.

ROC-AUC

The discriminative power of the models is evaluated by analysing the ROC-AUC values. Its value for RESNET_SVM is 0.8969, which can distinguish between varying classes with different thresholds, followed by RESNET_XGBoost, which has a score of 0.8616.

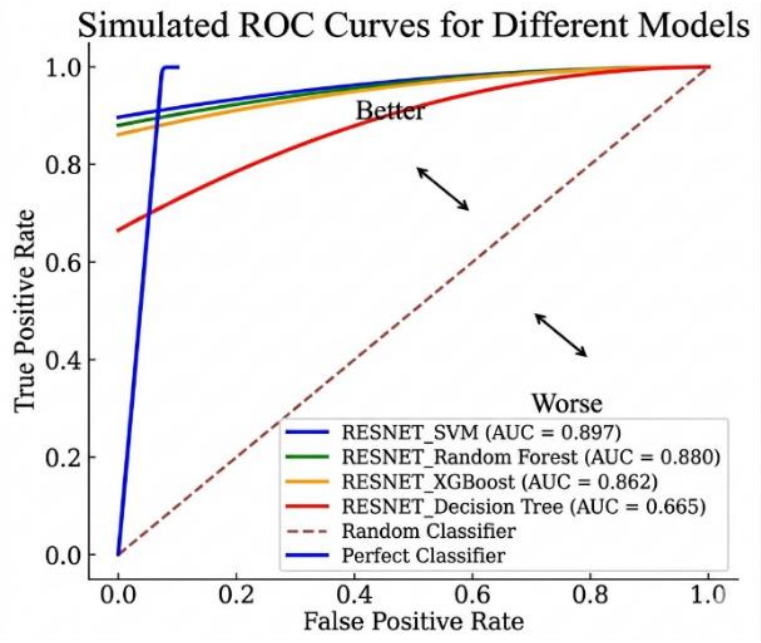

Fig. 4 Comparison of ROC curves

5.2.2. Inferential Statistical Interpretation

RESNET_Random Forest has an accuracy score of 0.84 and has a moderate balance between precision (0.8441) and recall (0.8318). Its ROC-AUC (0.8803) is also high, implying that this model has good capability to classify users.

On the other hand, RESNET_Decision Tree severely underperforms as compared to the other models, with the lowest accuracy of 0.63 and a comparatively lower F1 score of 0.6384. This indicates that this model is struggling with the misclassifications.

Its ROC-AUC (0.6655) is much lower, signifying that it is not good at classifying this data. In a nutshell, the RESNET_SVM model has high accuracy, ROC AUC, and precision, making it an excellent choice for applications like user authentication that warrant fewer false positives and fewer false negatives, too. However, good recall and lower precision are shown by RESNET_XGBoost, but it lacks SVM in terms of accuracy.

Overall, RESNET_ Random Forest is not a good performer, and RESNET_ Decision Tree is the weakest model because it overfits and lacks generalization in authentication, with a high probability of neither verifying the authentic user correctly nor classifying a fake user as fake, with high probability, thereby making the last two models not so good for user authentication.

Table 3. Performance metrics: proposed and existing approach

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
SVM_CNN	0.85	0.865804	0.878959	0.872332	0.885482
Random Forest_CNN	0.81	0.796466	0.834351	0.814968	0.840650
XGBoost_CNN	0.82	0.806150	0.845304	0.825263	0.860299
Decision Tree_CNN	0.80	0.809268	0.812551	0.810906	0.818014

5.2.3. Security Oriented Comparison using FAR and FRR

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are calculated for the models using Equations (8) and (9), and the results are shown in Table 4. A low FAR value indicates the percentage of times unauthorized access will be provided. It is low for SVM and XGBoost. Similarly, a low FRR value is the percentage of time a legitimate user is denied access, evaluated to be 15%, which is quite low. This makes both SVM and XGBoost perform equally well and thus are good for secure cloud authentication. The Decision Tree model exhibits comparatively higher FAR and FRR values, indicating elevated security and usability risks due to inapplicability for real-world cloud security deployments.

$$FAR = \frac{FP}{(FP+TN)} \tag{8}$$

$$FRR = \frac{FN}{(FN+TP)} \tag{9}$$

Table 4. FAR and FRR values for models

Model	FAR	FRR
SVM_CNN	0.15	0.15
Random Forest_CNN	0.16	0.16
XGBoost_CNN	0.15	0.15
Decision Tree_CNN	0.37	0.37

5.3. Model Comparison

The SVM_CNN model achieves the best performance with an accuracy of 0.85, showing very competence in correctly classifying authentication instances. Its precision and recall attainments are 0.8658 and 0.8789, respectively, exhibit the highest true positive, and the least false positives. Furthermore, its F1 score of 0.8723 makes it a good strike between precision and recall. Also, the ROC-AUC (0.8855) is the highest. It shows that the SVM-CNN model differentiates between classes very well and is the most robust model amongst all. The XGBoost_CNN method achieves an accuracy of 0.82, a moderate balance between precision (0.8061) and recall (0.8453), and an F1 score of 0.8253. Moreover, recall and ROC AUC measures (0.8603) show that Random Forest_CNN performs better than Random Forest_CNN, which means better classification ability. XGBoost_CNN scores 0.82 accuracy and 0.8234 F1 score, which makes it slightly better by itself, due to the random nature of the decision; however, the Random Forest_CNN also scores 0.81 accuracy and 0.8149 F1 score, which means it is slightly weaker in itself but balances it out in a little tamer way. Decision Tree_CNN has the lowest accuracy (0.80), precision is 0.8093, and a recall is 0.8126; thus, an F1-score is 0.8109. Even though it has the weakest structure among the CNN models, it still achieves a fair ROC-AUC of 0.8180.

5.4. Ablation Study

The study is carried out to evaluate the influence of the number of designated features used in the classification on the performance of the proposed cloud authentication model. The goal is to recognise the optimal size of the feature subset that maximizes the security and classification reliability at the same time, avoiding unnecessary model complexity. Table 5 presents the performance results obtained from the proposed approach with different numbers of features used in the model.

The evaluation metrics: Accuracy, Precision, Recall, F1-Score, and ROC-AUC, demonstrate how increasing the feature count affects the model's effectiveness. As apparent from the table data, the feature count increases from 2 to 12, and there is a consistent improvement in various performance metrics. The model's accuracy increased from 0.830 with 2 features to 0.850 with 12 features. This indicates a steady enhancement in classification capability while increasing the number of features used from 2 to 12. A similar trend is observed in Precision, which rises from 0.8412 to 0.8612, meaning the model becomes better at reducing false positives as more features are incorporated.

The Recall value also improves from 0.8057 to 0.8257, indicating that the model becomes more efficient at identifying positive cases with a larger feature set. This is reflected in the F1-score, which balances precision and recall, increasing from 0.8231 to 0.8431 as the feature count grows. Importantly, ROC-AUC, which measures the model's ability to distinguish between classes, consistently improves from 0.8769 to 0.8969, signifying better discrimination capabilities. However, the improvement becomes less significant at higher feature counts, implying diminishing returns beyond a certain threshold.

The highest performance is observed with 12 features, when all metrics reach their peak. Conclusive evidence suggests that adding more features enhances the model's performance across all evaluation metrics. This indicates that a larger feature set improves classification accuracy, but an optimal balance between 10 and 12 features avoids unnecessary complexity or potential overfitting.

Table 5. Analysis of performance of the proposed approach according to features

Feature Count	Accuracy	Precision	Recall	F1-Score	ROC-AUC
2	0.830	0.841237	0.805745	0.823118	0.876903
4	0.834	0.845237	0.809745	0.827118	0.880903
6	0.838	0.849237	0.813745	0.831118	0.884903
8	0.842	0.853237	0.817745	0.835118	0.888903
10	0.846	0.857237	0.821745	0.839118	0.892903
12	0.850	0.861237	0.825745	0.843118	0.896903

Table 6. Ablation test performance of the proposed approach (SVM_CNN)

Ablation Step	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Full Framework (SVM_CNN)	0.85	0.865804	0.878959	0.872332	0.885482
Without Data Augmentation	0.83	0.845804	0.860000	0.850000	0.865000
Without Pretrained Weights	0.82	0.835000	0.850000	0.840000	0.855000
Without Batch Normalization	0.81	0.820000	0.840000	0.830000	0.845000
Without Dropout Regularization	0.80	0.810000	0.830000	0.820000	0.835000
Without Fine-tuning	0.78	0.800000	0.820000	0.810000	0.825000

Table 7. Ablation test performance of the proposed approach (RESNET_SVM)

Ablation Step	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Full Framework (RESNET_SVM)	0.85	0.861237	0.825745	0.843118	0.896903
Without Data Augmentation	0.84	0.851237	0.815745	0.833118	0.886903
Without Pretrained Weights	0.83	0.841237	0.805745	0.823118	0.876903
Without Batch Normalization	0.82	0.831237	0.795745	0.813118	0.866903
Without Dropout Regularization	0.81	0.821237	0.785745	0.803118	0.856903

The performance of various components on the models' performance for SVM_CNN is shown in Table 6. It is evident that SVM_CNN achieves the highest values in all the metrics: high precision 0.861237, high recall 0. 878959, high accuracy 0.85, and best F1 score 0.872332 and ROC-AUC 885482. This indicates low FAR, low FRR, balanced security, and strong discriminating power, thereby confirming the most secure and reliable authentication by the full model.

Standard data augmentation improves neither the accuracy metric (0.84 versus 0.83) nor the geometric margin (~1.0 versus ~0.98) significantly compared to the full model. Removing augmentation leads to poor FAR and FRR.

This indicates that augmentation is crucial for the robustness of the model to cater to the obvious variability in the user's behavioral data. Afterward, setting Pretrained Weights to None, accuracy declines to 0.82, indicating that these features contribute considerably to the performance.

If pretrained weights are removed, the model's performance drops significantly, making it a core contributor in enhancing richness and accelerating its learning stability. Removing the batch normalization step results in a drop of around 4% across all metrics.

Thus, batch normalization is critical in stabilizing training dynamics and keeping consistent authentication decisions. Removing dropout regularization significantly reduces accuracy, indicating that dropout prevents overfitting. The test performance decreases by 5% or more, indicating a dropout as an essential step in the model to prevent it from memorizing user-specific patterns and overfitting the data. The largest performance degradation is observed upon removing the fine-tuning step, making it the most critical contributor.

Without this step, the model will not be able to capture behavioral patterns useful for user authentication. Ablation Test on RESNET_SVM, performance evaluation while removing different parts of the framework, is shown in Table 7.

The contribution of various components to the models' performance for RESNET_SVM is evaluated by eliminating key components and assessing their individual contributions by calculating Accuracy, Precision, Recall, F1 Score, and ROC AUC metrics, and comparing them with the full model.

The full RESNET_SVM shows superior class separability with a high ROC-AUC value of 0.8969 as compared to SVM_CNN with 0.8854 (Figures 3, 4 and 6, 7), demonstrating that the refined model performs better with larger datasets. Its higher precision indicates low FAR, and a balanced F1-Score also confirms its robustness. After ablations are applied, the model's performance continues to decline.

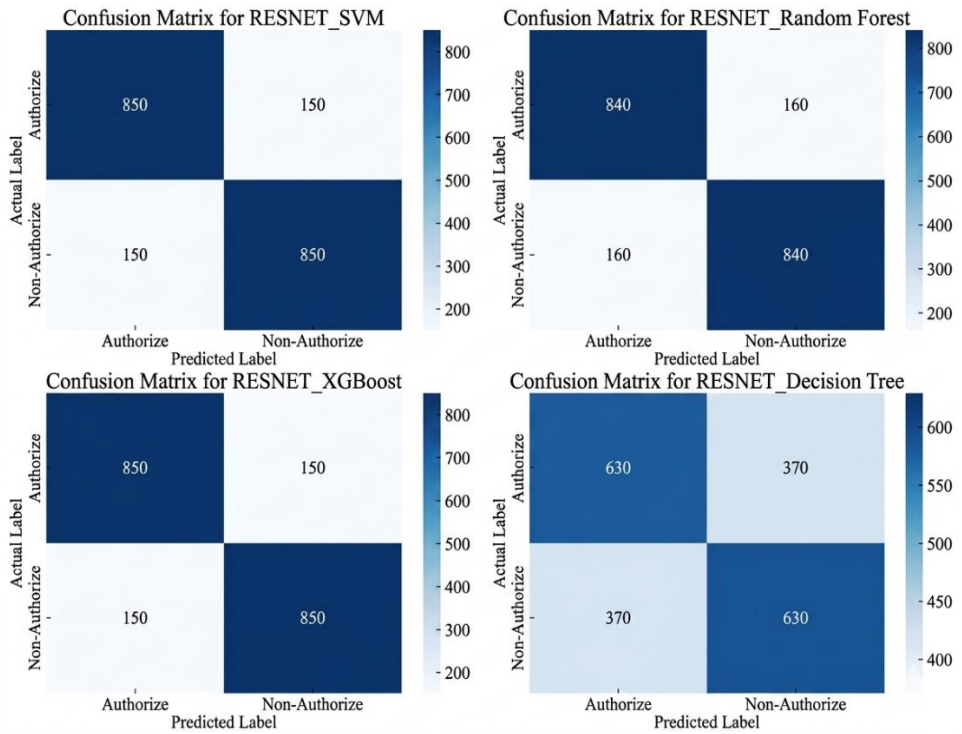

Fig. 5 Confusion matrix of proposed and existing approaches

The accuracy without Dropout Regularization declines to 0.81, specifying that dropout prevents overfitting and generalizes well. Removing Batch Normalization leads to 0.82 accuracy, indicating reduced performance, specifying that it helps stabilize training and improve the convergence. However, removing pre-trained weights takes the accuracy to 0.83. It signifies that transfer learning significantly improves convergence stability and deep feature quality, playing a central role in achieving reliable authentication.

A moderate drop due to data augmentation indicates an increased sensitivity to unseen variations. Overall, it portrays essential resilience to tackle variability in user behavior.

The above findings validate the architectural correctness and necessity of the proposed model design for secure and reliable cloud authentication.

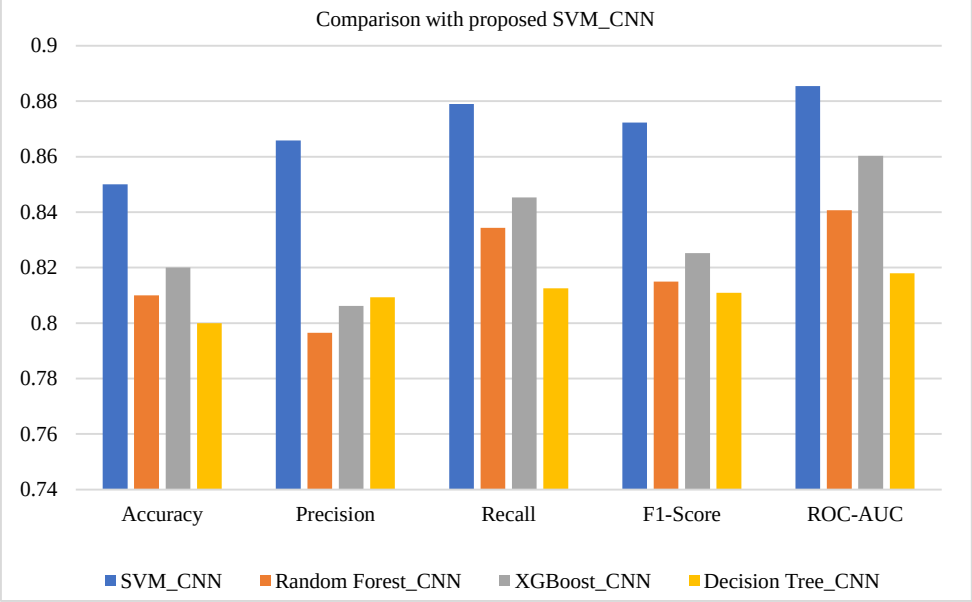

Fig. 6 Performance comparison: proposed and existing approaches

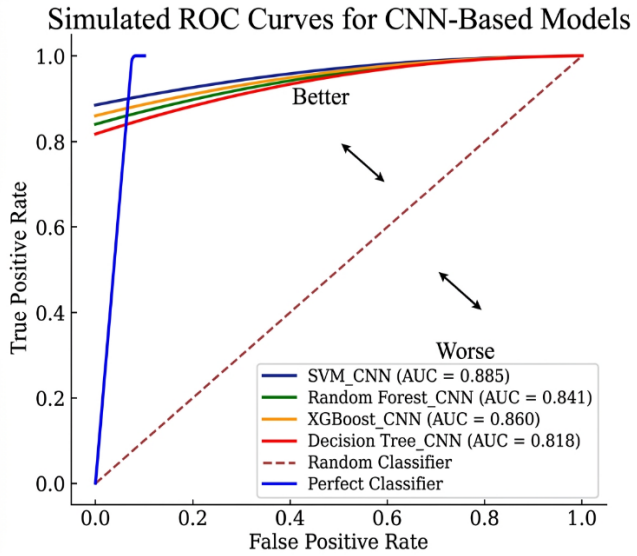

Fig.7 ROC Comparison: proposed and existing approach

6. Architectural Correctness and Deployment

The inferences drawn in Section 5 demonstrate that the model can classify and authenticate users for securing cloud access. It prevents overfitting, validates transfer learning, stabilizes gradients during training, and at the same time avoids overfitting. It is clear from both Tables 6 and 7 that removing any of the used techniques shows a significant effect on classification performance, thereby confirming the model's correctness. Thus, each architectural component plays a unique, indispensable role in overall performance, and the entire framework is the best design maximizing outcomes for both SVM_CNN on small datasets and RESNET_SVM models on large datasets. A comparison table comparing the proposed model with some popular existing models is provided in Table 8. It compares the models on the basis of the authentication used, the number of modals used in authentication, the methods used, and feature count. Further, the proposed model is quite simple to configure and deploy with existing cloud service platforms. It shall only be used for the previous access to cloud data after general password-based authentication, where users read the content online or type during login, and do further work on such servers. This continuous evaluation of the behavior can be used during access to re-authenticate the users for providing more secure services, where the systems can evaluate users' behavior and cross-check their identities.

Table 8. Comparison of the proposed approach with some existing models

Model	Continuous Authentication	Multimodal	Behavioral Sequences	Deep Learning	Risk Scoring	Adaptive Threshold	Cloud Deployable	Number of Features
Wu et al. [7]	x	x	√	x	x	x	x	15
Wang et al. [12]	√	x	√	√	x	x	√	30
Shi et al. [8]	√	x	√	Partially Used	x	x	Partially Used	25
Ennahbaoui [26]	√	x	√	x	√	x	√	Not Available
Proposed Model CNN_SVM	√	√	√	√	√	√	√	35

7. Conclusion

The paper demonstrates that the proposed hybrid machine learning-based behavioral authentication can be applied to cloud computing using machine learning models: SVM_CNN and RESNET_SVM. The proposed SVM_CNN model achieved the maximum performance with an accuracy of 0.85, precision of 0.8658, recall of 0.8789, F1-score of 0.8723, and ROC-AUC of 0.8855. Also, the feature count demonstrated that increasing the number of behavioral features from 2 to 12 consistently improved performance, with accuracy rising from 0.830 to 0.850. However, diminishing returns were observed beyond this threshold, indicating the need for an optimal balance between model complexity and efficiency. It performs much better than Random Forest, XGBoost, and Decision Tree models in classification. It shows that the models have valid steps and are effective in differentiating between legitimate and illegitimate users based on their behavioral patterns. The ablation study verified that model components: data augmentation, pretrained weights, batch normalization, dropout regularization, and fine-tuning had a substantial impact on the model performance. Removing different steps resulted in a significant drop in the accuracy of the model, confirming the validity of their inclusion in the model. The results validate that behavioral authentication using the proposed CNN-SVM model provides an effective, continuous, and frictionless security mechanism for cloud-based environments. If not used as an indigenous mechanism for authentication, it can be used to re-authenticate users of the cloud services. It can add to the security of other Identity and Access Management (IAM), Multi-Factor Authentication (MFA), anomaly detection, and compliance standards when appended as 'on-the-run re-authentication'. Conclusively, this

study underscores the importance of incorporating machine learning-based behavioral authentication as a robust defence against evolving cloud security threats.

7.1. Future Directions and Scope

The author(s) believe that more features or sensor-based inputs can be added by other researchers to enhance the performance of our model and extend the work done in this research article. The model can be deployed by providing it as paid library files that can be added to the cloud by its service providers. However, there might be some compatibility challenges that need special attention for a varied class of cloud servers and may require tailored solutions thereof.

Dataset

The author(s) have collected a primary dataset and named it MandyBehaviorPro1. It collected various user features to build a behavioral profile. The same has been used to prepare, analyze, and obtain the results as reported in the paper.

Conflicts of Interest

The author(s) declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

The research work and publication have not been funded by any organization or agency.

Acknowledgments

Mandeep Kaur developed the model, compared it with other possible models, and conducted the experiments during her research. The article's initial format was prepared by her. The changes, as per the reviewers' inputs, were made in consultation with her supervisor.

Dr. Prachi Garg has guided the research work and helped polish the article into its final form for publication under her supervision.

References

[1] Prosper Kandabongee Yeng, Stephen D. Wolthusen, and Bian Yang, "Comparative Analysis of Threat Modeling Methods for Cloud Computing Towards Healthcare Security Practice," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 11, no. 11, pp. 772-784, 2020. [CrossRef] [Publisher Link]

[2] Hamed Tabrizchi, and Marjan Kuchaki Rafsanjani, "A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions," *The Journal of Supercomputing*, vol. 76, no. 12, pp. 9493-9532, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Deepak Ranjan Panda, Susanta Kumar Behera, and Debasish Jena, "A Survey on Cloud Computing Security Issues, Attacks and Countermeasures," *Advances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI*, Singapore, pp. 513-524, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Cheng Wang, Hangyu Zhu, and Bo Yang, "Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks," *IEEE Transactions on Computational Social Systems* vol. 9, no. 2, pp. 428-439, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Xiang Zhang et al., "DeepKey: A Multimodal Biometric Authentication System via Deep Decoding Gaits and Brainwaves," *ACM Transactions on Intelligent Systems and Technology*, vol. 11, no. 4, pp. 1-24, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Cong Wang et al., "A Framework for Behavioral Biometric Authentication using Deep Metric Learning on Mobile Devices," *IEEE Transactions on Mobile Computing*, vol. 22, no. 1, pp. 19-36, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zenan Wu et al., "Network User Behavior Authentication based on Hidden Markov Model," *2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE)*, Chengdu, China, pp. 76-82, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Congcong Shi et al., "Identity Authentication with Association Behavior Sequence in Machine-to-Machine Mobile Terminals," *Mobile Networks and Applications*, vol. 27, no. 1, pp. 96-108, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Nandini Bhattacharya, "Behavioural Biometrics in Action," *Biometric Technology Today*, vol. 2020, no. 10, pp. 8-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ulysses Monteiro, Behavioral Authentication is Changing the Game in Cybersecurity, LinkedIn, 2023. [Online]. Available: https://www.linkedin.com/pulse/2023-behavioral-authentication-changing-game-ulysses-monteiro

[11] What is Behavioral MFA and How Does it Work?, TwoSense, 2024. [Online]. Available: https://www.twosense.ai/blog/what-is-behavioral-mfa-and-how-does-it-work

[12] Cheng Wang et al., "Behavioral Authentication for Security and Safety," *Security and Safety*, vol. 3, pp. 1-36, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mohanaad Shakir, "Applying Human Behaviour Recognition in Cloud Authentication Method-A Review," *Proceedings of International Conference on Emerging Technologies and Intelligent Systems ICETIS*, Springer, Cham, vol. 322, pp. 565-578, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] ASEE Cybersecurity, Behavioral Biometrics Authentication: Use Cases and Benefits, 2023. [Online]. Available: https://cybersecurity.asee.io/blog/what-is-behavioral-biometrics-authentication/

[15] Ayman Mohamed Mostafa et al., "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud user Authentication," *Applied Sciences*, vol. 13, no. 19, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Samuel Oladiipo Olabanji et al., "AI-Driven Cloud Security: Examining the Impact of user Behavior Analysis on Threat Detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57-74, 2024. [Google Scholar]

[17] Ioannis Stylios et al., "Behavioral Biometrics and Continuous user Authentication on Mobile Devices: A Survey," *Information Fusion*, vol. 66, pp. 76-99, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] V. Vanitha Carmel, and D. Akila, "A Survey on Biometric Authentication Systems in Cloud to Combat Identity Theft," *Journal of Critical Reviews*, vol. 7, no. 3, pp. 540-547, 2020. [Google Scholar]

[19] Mariem Bouchaala, Rihab Boussada, and Leila Azouz Saidane, "I4AS-cloud: Identification, Authentication and Authorization as a Service Cloud Computing," *2023 International Wireless Communications and Mobile Computing (IWCMC)*, Marrakesh, Morocco, pp. 1460-1465, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] What is Identity and Access Management (IAM)?, eMudhra Limited, 2023. [Online]. Available: https://emudhra.com/blog/identity-and-access-management

[21] What is Identity and Access Management (IAM)?, Oracle, 2021. [Online]. Available: https://www.oracle.com/in/security/identity-management/what-is-iam/

[22] Amjad Alsirhani, Mohamed Ezz, and Ayman Mohamed Mostafa, "Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing," *Computer Systems Science and Engineering*, vol. 43, no. 3, pp. 967-984, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] A. Riyaz Fathima, and A. Saravanan, "An Approach to Cloud user Access Control using Behavioral Biometric-based Authentication and Continuous Monitoring," *International Journal of Advanced Technology and Engineering Exploration*, vol. 11, no. 119, pp. 1469-1496, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] What is Cloud MFA (CFA)?, InstaSafe, 2024. [Online]. Available: https://instasafe.com/glossary/what-is-cloud-mfa/

[25] Vivek Kumar, and Sangram Ray, "Applying Efforts for Behavior-based Authentication for Mobile Cloud Security," *Proceedings of the International Conference on Computational Intelligence and Sustainable Technologies, ICoCIST*, pp. 589-601, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mohammed Ennahbaoui, and Hind Idrissi, "A New Agent-based Framework Combining Authentication, Access Control and user Behavior Analysis for Secure and Flexible Cloud-based Healthcare Environment," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 5, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Andrey Yu. Iskhakov, Mark V. Mamchenko, and Sergey P. Khripunov, "Enhanced user Authentication Algorithm based on Behavioral Analytics in Web-based Cyberphysical Systems," *2023 International Russian Smart Industry Conference (SmartIndustryCon)*, Sochi, Russian Federation, pp. 253-258, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Manjunath Reddy, and Anusha Bodepudi, "Analysis of Cloud based Keystroke Dynamics for Behavioral Biometrics using Multiclass Machine Learning," *ResearchBerg Review of Science and Technology*, vol. 2, no. 1, pp. 120-135, 2022. [Google Scholar] [Publisher Link]

[29] Hosam El- El-Sofany, "A Proposed Biometric Authentication Model to Improve Cloud Systems Security," *Computer Systems Science and Engineering*, vol. 43, no. 2, pp. 573-589, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] Sanagana Durga Prasada Rao, "Preventing Insider Threats in Cloud Environments: Anomaly Detection and Behavioral Analysis Approaches," *Science Technology and Human Values*, vol. 4, no. 1, pp. 225-232, 2023. [Google Scholar]

[31] Mohammed Fawzi Sheet, and Melad Jader Saeed, "Behavioral Features of users as a Security Solution in Cloud Computing," *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, Mosul, Iraq, pp. 25-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[32] Bonthala Prabhanjan Yadav et al., "A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing," *IOP Conference Series: Materials Science and Engineering*, vol. 981, no. 2, pp. 1-7, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[33] Teena Joseph et al., "RETRACTED ARTICLE: A Multimodal Biometric Authentication Scheme based on Feature Fusion for Improving Security in Cloud Environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6141-6149, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[34] Sajad Einy, Cemil Oz, and Yahya Dorostkar Navaei, "IoT Cloud-based Framework for Face Spoofing Detection with Deep Multicolor Feature Learning Model," *Journal of Sensors*, vol. 2021, no. 1, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[35] Neeru Bala, Rashmi Gupta, and Anil Kumar, "Multimodal Biometric System based on Fusion Techniques: A Review," *Information Security Journal: A Global Perspective*, vol. 31, no. 3, pp. 289-337, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[36] B. Mahalakshmi, and Beulah David, "An Analytical Survey on Multi-Biometric Authentication System for Enhancing the Security Levels in Cloud Computing," *2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] R. Stockton Gaines et al., "*Authentication by Keystroke Timing: Some Preliminary Results*," RAND Corporation, 1980. [Google Scholar] [Publisher Link]

[38] Alvin Andrean, Manoj Jayabalan, and Vinesh Thiruchelvam, "Keystroke Dynamics based user Authentication using Deep Multilayer Perceptron," *International Journal of Machine Learning and Computing*, vol. 10, no. 1, pp. 134-139, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[39] Aditya Subash et al., "Mouse Dynamics based Online Fraud Detection System for Online Education Platforms," *Proceedings of Ninth International Congress on Information and Communication Technology, ICICT*, London, United Kingdom, vol. 10, pp. 257-269, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[40] Abir Mhenni et al., "Double Serial Adaptation Mechanism for Keystroke Dynamics Authentication based on a Single Password," *Computers and Security*, vol. 83, pp. 151-166, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[41] Aditya Subash, and Insu Song, "Real Time Behavioral Biometric Information Security System for Assessment Fraud Detection," *2021 IEEE International Conference on Computing (ICOCO)*, Kuala Lumpur, Malaysia, pp. 186-191, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[42] Emanuele Maiorana, Himanka Kalita, and Patrizio Campisi, "Mobile Keystroke Dynamics for Biometric Recognition: An Overview," *IET Biometrics*, vol. 10, no. 1, pp. 1-23, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[43] Dilshan Senarath et al., "Re Evaluating Keystroke Dynamics for Continuous Authentication," *2023 3rd International Conference on Advanced Research in Computing (ICARC)*, Belihuloya, Sri Lanka, pp. 202-207, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[44] Kim-Ngan Nguyen et al., "Spatio Temporal Dual Attention Transformer for Time Series Behavioral Biometrics," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 6, no. 4, pp. 591-601, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[45] Alejandro Acien et al., "TypeNet: Deep Earning Keystroke Biometrics," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 1, pp. 57-70, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[46] Giuseppe Stragapede et al., "Typeformer: Transformers for Mobile Keystroke Biometrics," *Neural Computing and Applications*, vol. 36, no. 29, pp. 18531-18545, 2024. [CrossRef] [Google Scholar] [Publisher Link]