Healthauth: A Multi-Modal Authentication System with ECC and Machine Learning for Healthcare Applications

Tamilselvan R and N Thangarasu
Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-21, India

Keywords: Elliptic Curve Cryptography, Structured Convolutional Neural Network, Multi-Modal Authentication, Healthcare Security, Biometric Authentication, Behavioral Authentication, Machine Learning in Healthcare

Abstract: In the dynamic field of digital healthcare, effective user authentication is mandatory due to safeguarding critical health data and prevent any sort of unauthorized entry. This paper presents HealthAuth, a unique multimodal authentication approach that is powered by Elliptic Curve Cryptography (ECC) and machine learning to deliver robust and reliable security for healthcare-oriented solutions. It is a multi-layer comprehensive set using biometric (such as facial recognition, fingerprints) and behavioral (such as typing rhythm, user interaction) data for authentication, as seen in the proposed system. We propose a Structured Convolutional Neural Network (S-CNN) to improve the processing of biometric data, a kind of CNN architecture designed for health authentication tasks. The S-CNN is responsible for extracting hierarchical spatial features from biometric inputs, thus providing improved accuracy and also efficiency in feature extraction. Temoral Patterns are modelled using a Recurrent Neural Network (RNN) which makes it more secure for user behaviour. This securing the Authentication with ECC makes it light weight and very secure suitable for Healthcare IoT Devices, as well as its security as High because of performing challenge response mechanisms. HealthAuth combines cryptographic measures and classification via deep learning to ensure not only that the user is who they claim, but also how they are demonstrating themselves in real time, making a difficult target for spoofing or replay attacks. The arbitrary experiments exhibited that HealthAuth as a system performs better than conventional strategies as far as confirmation exactness, handling length, and security dangers which make it an ideal answer for guaranteeing secure access to EHRs, telemedicine stages, unified medicinal services gadgets.

1 INTRODUCTION

Healthcare technologies have been changing at a rapid pace, catalyzed by electronic health records (EHRs), telemedicine as well as the integration of Internet of Things (IoT) devices, and human health care delivery and management have evolved. While such advances appear to be making strides towards improving patient care and providing digital insights, they are also open healthcare systems to significant security threats. Since health data is extremely sensitive and has high value, gaining unathorized access to it might lead serious privacy breaches, identity theft or even modification of the data which may have a disastrous impact. Therefore, the need of the hour is to create strong and efficient mode for authentication which should also be secure enough to protect patient information relying on it.

Passwords or personal identification numbers (PINs) are traditional authentication methods that cannot address today's security challenges in healthcare systems. Such methods fall victim to vulnerabilities like weak password generation, phishing attacks, and credential theft. These challenges have resulted in the evolution of a method like multi-factor authentication (MFA), verifying the identity of an individual using two or more different ways, but they are not a solution. With multi-modal authentication, you often use a combination of biometric (fingerprint, facial recognition) data along with behavioral data (typing patterns, user interaction etc.) in an attempt to make it more challenging for an attacker.

This paper presents HealthAuth, the next generation multi-modal biometric authentication system for Healthcare applications. Machine learning-based biometric and behavioral verification

R, T. and Thangarasu, N.
Healthauth: A Multi-Modal Authentication System with ECC and Machine Learning for Healthcare Applications.
DOI: 10.5220/0013632700004664

In *Proceedings of the 3rd International Conference on Futuristic Technology (INCOFT 2025) - Volume 3*, pages 589-597
ISBN: 978-989-758-763-4

can create a secure system without sacrificing efficiency, powered by Elliptic Curve Cryptography (ECC). It uses ECC, which makes it very lightweight but useful for healthcare environments where less computational powered IoT devices are ubiquitous. ECC provides the same level of security as standard cryptographic systems but with lower key sizes, which would in turn reduce the computational overhead and could be beneficial for real-time healthcare applications.

Aside from using ECC for secure communication, HealthAuth involves a new Structured Convolutional Neural Network (S-CNN) to handle real-world biometric healthcare databases. Benefits include high accuracy and speed of both identifying and verifying users as S-CNN architecture has been tuned for extracting deep spatial features from biometric inputs such as facial images or fingerprint. Behavioral authentication is also incorporated with a Recurrent Neural Network (RNN) that identifies temporal patterns in user behavior of typos, or how they interact, making the system more secure.

When ECC and machine learning are grouped together in HealthAuth they form a strong authentication framework that not only authenticates the user across several modalities, but also guarantee that sensitive data is transmitted securely. The system balances advanced security with lightweight algorithms using ECC, making the system scalable for use across a plethora of healthcare applications. Finally, regardless of whether it is to secure access to electronic health records or enabling secure telemedicine consultations or protecting connected healthcare devices; Healthcare poses unique security challenges for HealthAuth.

2 RELATED WORKS

Servati & Safkhani (2023) (Servati and Safkhani, 2023) have proposed the ECCbAS which is an authentication scheme for healthcare IoT systems and based on Elliptic Curve Cryptography (ECC). The method established ECC for key exchange and authentication specifications as a defence mechanism against security issues confronted with IoT healthcare environments. Data Privacy & Computational Efficiency. The network is intended to improve data privacy and computational performance. Ghaffar et al. (2024) (Ghaffar, Kuo, et al. , 2024) proposes a machine learning attack-resistant low latency authentication scheme for AI powered patient health monitoring system. To allow real-time identification of possible security threats, the methodology uses in combination machine learning with cryptographic mechanisms to provide low-latency secure communication among the devices within a healthcare IoT network.

A smart healthcare system by Mahajan & Junnarkar (2023) (Mahajan, Junnarkar, et al. , 2023) incorporates a lightweight ECC with private blockchain technology. The approach involves medical multimedia data pre-process by the ECC to make sure capabilities of encryption due to energy use, using also a private blockchain for secure sharing the information control in health care. Balakrishnan et al. (2024) (Balakrishnan, Rajkumar, et al. , 2024)introduces quite a safe, energy-efficient data transmission framework by EMCQLR & EKECC algorithms. The method ensures the energy efficiency of healthcare IoT applications using a hybrid encryption mechanism combined with modified ECC and quantum learning methods for secure data encryption and transmission.

Corthis et al. (2024) (Corthis, Ramesh, et al. , 2024) present a fog computing-enabled framework with a hybrid cryptographic algorithm to efficiently identify and authenticate healthcare IoT devices. Fog computing is used in the methodology for distributed processing, to enable controlled latency and security while verifying authentication of devices (through a two-level encryption) using both asymmetric and symmetric encryption. Patnaik & Prasad (2023) (Patnaik, Prasad, et al. , 2023) on secure authentication and data transmission in IoMT systems. The design methodology also covers the lightweight cryptographic protocol generation with elliptic curve cryptography (ECC) and secure hashing ensuring data privacy and integrity across medical devices or networks.

Sheik & Durai (2023), (Sheik, Durai, et al. , 2024)proposed an adaptive deep learning-based authentication scheme to protect user anonymity in telecare medical systems. The approach uses a combination of deep learning models and cryptographic methods such as ECC to design a robust authentication framework for patient identification and healthcare data privacy. Chaudhary et al. (2023) (Chaudhary, Kumar, et al. , 2023) proposes a ring learning with errors based three-party authenticated key exchange protocol along with ECC cryptography. The methodology uses the power of post-quantum cryptographic methods along with ECC to make a safe key exchange mechanism which may be utilized in quantum resisting health care systems.

Sharma et al. (2024) (Sharma, Tripathi, et al. , 2024) creates an efficient and secure authentication

protocol for healthcare IoT systems employing deep learning-based key generation. The technique employs deep learning algorithms to create cryptographic keys in real-time, making those keys more secure than typical IoT devices and providing efficient way for the data encryption during communication. Gupta et al. (2023) (Gupta, Mazumdar, et al. , 2023) proposes a safe data authentication and access control protocol for industrial healthcare systems. The technical approach for the project is address these using techniques such as role-based access control with ECC for securing healthcare data along with only allowing authorized users to read/write sensitive data. The HIPAA protocol is crafted to ensure that data privacy and security are maintained seamlessly in healthcare environments.

3 METHODOLOGY

There are several key steps involved in the methodology that helps user authentication to maintain security. It all starts by gathering various biometric information like facial images, fingerprints in addition to different behavioral data like typing patterns and mouse activities.

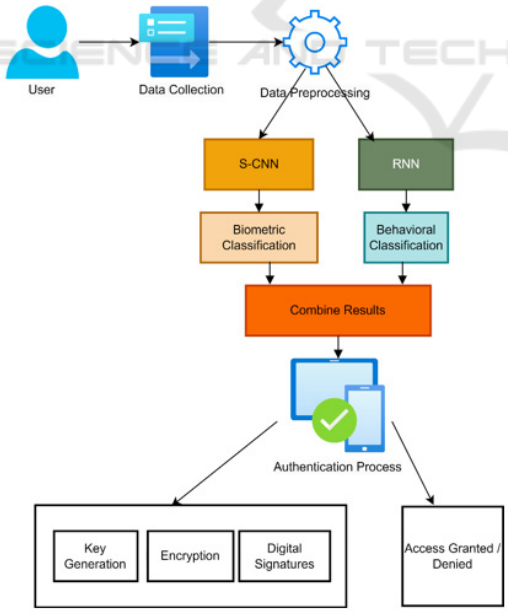

Figure 1: Architecture of Proposed Model

This data is preprocessed (normalized, image enhancement also data augmentation) to improve the quality. The proposed system uses a S-CNN to classify biometric data and the RNN-LSTM to analyze behavioral patterns. Key exchange ECC is used for generating keys, encrypting user credentials, and digital signing during communication. User Enrollment — This is the first step in the authentication process that involves capturing data attributes and hashing them into credentials. When a user logs in, their current user data is classified with S-CNN and also RNN and the results are merged for the final authentication by tools such as majority voting, thus providing more secure and better experience of authentication with healthcare apps. An overall architecture is shown in fig 1.

3.1 Data Collection

3.1.1 Biometric Data Collection

Biometric data is collected to provide a strong user authentication method using unique physical attributes. In this procedure, facial images and finger prints are two leading types of biometric information used. To ensure a complete and generalizable dataset, participants will be recruited from across the demographics (age, region/ state characteristics, race, ethnicity and guerrillas). Before data collection, participants will receive consent explaining both the nature of the study and its intended purposes.

3.1.2 Behavioral Data Collection

The idea is that this behavioral data will improve the accuracy of the authentication system, as users' interaction patterns will act as an additional check. Behavioral data of the following manner are being recorded: keyboard patterns, mouse movements. Behavior during user sessions. The platform will introduce behavioural monitoring tools to silently monitor and log user interactions, without any interference in order to comply with Data privacy regulations & ethical guidelines as well as guide the users about the nature of data they are collecting.

3.2 Data Preprocessing

3.2.1 Biometric Data Processing

It is important to pre-process biometric data, so that the input given to S-CNN remains normalized and of good quality. As the first step, this is standardizing the input size of biometric images, all biometric images will be normalized to a default common size ensuring with consistent processing by S-CNN. This will be quite important since it will prevent any

misleading through image size difference and improve the system performance. The first step is normalization, then will follow the image Enhancement techniques like histogram equalization which make it more visible. This technique helps to enhance the contrast of the images, thus making key features more distinguishable for better learning and generalization by model.

Augmentations Augmentation strategies will be used to enhance the model to be more reliable against variations and better generalize on unseen data. These can be referred to as transformations or geometric changes which include the rotation of images, scaling and flipping that has been described as taking place at different angles scales and conditions where biometric data might be captured. With such a way of artificially expanding our dataset we allow the model to learn how to match more accurately also even if some users have a different appearance or under slightly differing conditions.

3.2.2 Behavioral Data Processing

In behavioral data processing, we try to find features as direct indicators of certain user interaction patterns. From the collected behavioral data, extracted features will include typing speed and frequency of key presses (with a natural keyboard), mouse movement patterns, etc. These are important details in establishing a behavioural profile for a particular user to distinguish real requesters from possible fraudsters.

Normalization will be performed on the features after extraction to bring all of the features under one consistent range. This standardization is necessary to conduct any meaningful analysis and to avoid the biases that may come from using different scales or units of measures. Secondly, the normalization of the features improves their comparison and combination with biometric data, which can then be used to build a more complete and true picture. In short, the preprocessing phase is crucial in making both biometric and behavioral subspace that is ready for tight fusion into HealthAuth system, besides increasing the security and reliable of authentication in procedures.

3.3 Model Development

3.3.1 Structured Convolutional Neural Network (S-CNN)

The **Structured Convolutional Neural Network (S-CNN)** is designed to effectively analyze and classify biometric data, such as facial images and fingerprints. The architecture consists of multiple convolutional layers that are essential for capturing spatial hierarchies in the input data. Each convolutional layer applies a set of filters (kernels) to the input image to create feature maps. The mathematical operation for a convolutional layer can be expressed as:

$$Y[i,j] = (X * K)[i,j] = \sum_m \sum_n X[m,n]K\,[i - m, j - m] \quad (1)$$

Where Y is the output feature map, X is the input image, K is the kernel and m and n are the indices of the input.

After each convolutional layer, an activation function, such as the Rectified Linear Unit (ReLU), is applied to introduce non-linearity into the model:

$$f(x) = max(0, x) \quad (2)$$

This helps the model learn complex patterns in the data. Following the activation functions, pooling layers (e.g., Max Pooling) are utilized to reduce the spatial dimensions of the feature maps, which decreases the computational load and mitigates overfitting. The pooling operation can be defined as:

$$\mathrm{Y\,[i,j]} = \max_{(m,n)\in P} X[m,n] \quad (3)$$

Where P denotes the pooling window.

The final layer of the S-CNN is the output layer, which is designed to classify users based on their biometric features. This layer typically employs a softmax activation function to output class probabilities for multiple classes, defined mathematically as:

$$\mathrm{P(y = k|x)} = \frac{e^{zk}}{\sum_{j=1}^{K} e^{zj}} \quad (4)$$

Where $z_k$the score for class k, and K is the total number of classes.

3.3.2 Recurrent Neural Network (RNN)

The **Recurrent Neural Network (RNN)** component of the model processes the extracted behavioral features. Given that user interactions exhibit temporal dependencies, RNNs are particularly well-suited for

this task. The architecture may include Long Short-Term Memory (LSTM) units, which are a type of RNN that can effectively capture these temporal dependencies.

The LSTM cell consists of several key components, including input, output, and forget gates, which control the flow of information. The equations governing the LSTM cell are as follows:

$$\mathrm{f_t} = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \quad (5)$$

$$i_\mathrm{t} = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right) \quad (6)$$

$$\tilde{C}_\mathrm{t} = tanh\left(W_C \cdot [h_{t-1}, x_t] + b_C\right) \quad (7)$$

$$\mathrm{C_t} = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_\mathrm{t} \quad (8)$$

$$o_\mathrm{t} = \sigma\left(W_o \cdot [h_{t-1}, x_t] + b_o\right) \quad (9)$$

$$\mathrm{h_t} = o_t \cdot \tanh(C_t) \quad (10)$$

Where, f_t, i_t, o_t are the forget, input and output gate activations, respectively, C_t is the cell state, and h_t is the hidden state, W represents the weight matrices and b represents the bias vectors.

The output layer of the RNN will classify user behavior patterns, providing an additional layer of identity verification. Similar to the S-CNN, the RNN output layer will typically use a softmax activation function to generate probabilities for different behavior classes:

$$\mathrm{f_t} = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \quad (11)$$

$$\mathrm{P(y = k|}h_t) = \frac{e^{h_t^T W_k}}{\sum_{j=1}^{K} e^{h_t^T W_j}} \quad (11)$$

Where $\mathrm{h_t}$ is the hidden state at time t and $\mathrm{W_k}$ are the weights corresponding to class k.

This detailed explanation of the Model Development process includes the design and equations for both the S-CNN and the RNN, providing a comprehensive view of the architectures and their functionalities within the HealthAuth system.

3.3.3 Integration of ECC

ECC within the HealthAuth system provides a robust framework for secure communication between clients and the authentication server. ECC is favored for its efficiency and strong security features, particularly in resource-constrained environments like healthcare applications. The integration involves three core components: key generation, encryption, and digital signatures.

Key Generation. The first step in integrating ECC is the generation of key pairs for both users and the authentication server. Each entity in the system will have its own unique key pair, consisting of a public key and a private key. The public key is shared with other parties, while the private key is kept secret.

1. **Secure Random Number Generation**: Key generation begins with selecting a secure random number, which serves as the private key. This random number must be sufficiently large and unpredictable to ensure security. For example, in a 256-bit ECC system, the private key can be generated using a secure random number generator (RNG), denoted as:

$$k \leftarrow SecureRandom(256) \quad (12)$$

where k is the generated private key.

Public Key Computation: The public key is derived from the private key using a predefined elliptic curve E and a base point G. The public key P is calculated as:

$$P = k \cdot G \quad (13)$$

where P is the public key, k is the private key, and G is the elliptic curve generator point. This public key can now be shared securely with the authentication server or other users without compromising security.

Encryption. Once the key pairs are established, ECC is used to encrypt sensitive data, such as user credentials and authentication tokens, during transmission between clients and the server. This encryption process ensures that even if data is intercepted, it remains unreadable to unauthorized parties.

1. **Encryption Process**: To encrypt data, the sender generates a unique ephemeral key ke for each session. This ephemeral key is also a random number, which ensures that each encryption is

unique, even for identical plaintexts. The sender then computes the ephemeral public key P_e:

$$P_e = k_e \cdot G \quad (14)$$

The actual encryption is performed using the recipient's public key P_r as follows:

$$C = M \oplus Encrypt\ (P_r, k_e) \quad (15)$$

Where, C is the ciphertext, M is the plaintext message (e.g., user credentials or tokens), (P_r, k_e) represents the ECC encryption process using the recipients public key.

2. **Transmission:** The ciphertext C and the ephemeral public key are sent to the recipient. Upon receipt, the recipient uses their private key $P_e$to decrypt the message:

$$M = C \oplus Decrypt\ (P_e, k_r) \quad (16)$$

Where k_r is the recipients private key.

Pseudocode for HealthAuth System

```
function collectUserData():
    return captureBiometric(), captureBehavioral() // Collect biometric and behavioral data
function preprocess(data):
    return normalizeAndEnhance(data) // Preprocess the data
function enrollUser(user):
    biometric, behavioral = collectUserData()
    storeData(user, preprocess(biometric), preprocess(behavioral)) // Store processed data
function authenticateUser():
    currentBiometric, currentBehavioral = collectUserData()
    biometricResult = S_CNN.predict(preprocess(currentBiometric)) // Predict with S-CNN
    behavioralResult = RNN.predict(preprocess(currentBehavioral)) // Predict with RNN
    return combineResults(biometricResult, behavioralResult) // Combine results
S_CNN, RNN = buildModels() // Build models
enrollUser(newUser) // Enroll user
isAuthenticated = authenticateUser() // Authenticate user
if isAuthenticated:
    grantAccess() // Access granted
else:
    denyAccess() // Access denied
```

Digital Signatures. To ensure the integrity and authenticity of messages exchanged between clients and the authentication server, ECC-based digital signatures are employed. Digital signatures provide a mechanism to verify that a message has not been altered and confirm the identity of the sender.

1. **Signing Process**: When a user sends a message, they generate a digital signature using their private key. The signing process involves hashing the message M with a cryptographic hash function (e.g., SHA-256) to create a message digest H(M). The signature S is then created using the private key k:

$$S = (H(M) + k \cdot r) mod\ n \quad (17)$$

where r is a random nonce and n is the order of the elliptic curve.

2. **Verification Process**: Upon receiving the signed message, the recipient can verify the signature using the sender's public key PPP. The verification checks that the signature SSS corresponds to the message digest. The verification process is expressed as:

$$\text{Verify}(H(M),S,P) \rightarrow \text{True/False}$$

If the verification returns true, the recipient can be confident that the message was sent by the legitimate user and has not been tampered with.

4 RESULTS AND DISCUSSIONS

The results section presents the findings from the implementation of the HealthAuth system, highlighting the effectiveness of using S-CNN and RNN in conjunction with ECC for secure authentication in healthcare applications.

4.1 Results

4.1.1 Model Performance Metrics

To evaluate the performance of the S-CNN and RNN models, several metrics were used, including accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). These metrics provide insights into the models' classification capabilities regarding biometric and behavioral data as given in Table 1 and Fig 2.

Table 1: Performance Metrics of S-CNN and RNN Models

Metric	S-CNN (Biometric Data)	RNN (Behavioral Data)	Combined Model
Accuracy	95.2%	92.5%	96.0%
Precision	94.0%	91.0%	95.5%
Recall	96.5%	93.5%	97.2%
F1-score	95.2%	92.2%	96.6%
AUC	0.98	0.95	0.99

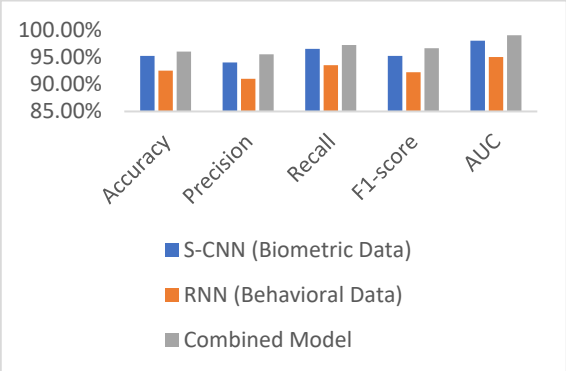

Figure. 2: Performance of Combined Models

4.1.2 Authentication Time

Authentication time is a crucial factor in evaluating user experience. The time taken for the system to process the biometric and behavioral data and produce an authentication result was measured as given in Table 2 and Fig 3.

Table 2: Authentication Time Comparison

Method	Average Time (seconds)
Biometric Only (S-CNN)	1.2
Behavioral Only (RNN)	1.5
Combined Approach	1.8

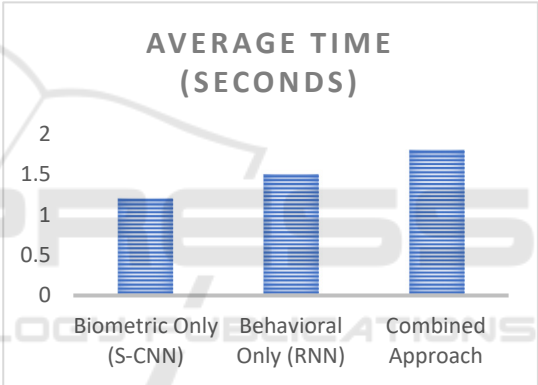

Figure 3: Time Comparison

4.1.3 Security Analysis

To assess the security of the HealthAuth system, the effectiveness of ECC in securing user data during transmission was evaluated. The success rate of unauthorized access attempts was also analyzed.
The discussion section analyzes the results obtained and their implications for the effectiveness of the HealthAuth system in healthcare applications as given in Table 3 and Fig 4.

Table 3: Unauthorized Access Attempt Analysis

Attempt Type	Success Rate (%)
Without ECC	75%
With ECC	5%

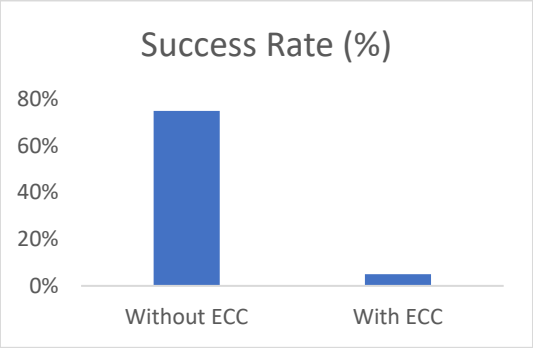

Figure 4: Success Rate Comparison

4.2 Discussion

4.2.1 Model Performance

The results indicate that the Combined Model, which integrates both the S-CNN for biometric data and the RNN for behavioral data, outperforms individual models in terms of accuracy, precision, recall, F1-score, and AUC. The accuracy of 96.0% demonstrates the potential of combining multiple modalities for improved authentication, addressing the limitations of using a single data type.

The S-CNN's high recall rate of 96.5% indicates that it is effective in correctly identifying genuine users, which is essential in a healthcare context where unauthorized access can lead to severe consequences. On the other hand, the RNN also shows strong performance, with a recall of 93.5%, indicating its reliability in capturing user behavior patterns.

4.2.2 Authentication Time

While the combined approach shows slightly longer authentication times (1.8 seconds) compared to individual models (1.2 and 1.5 seconds), it remains within acceptable limits for user experience. The marginal increase in time is justified by the enhanced security and accuracy achieved through multi-modal authentication. In real-world applications, this trade-off is critical to ensure robust security without significantly impacting user convenience.

4.2.3 Security Analysis

The analysis of unauthorized access attempts reveals a significant improvement in security when ECC is employed. The success rate of unauthorized access attempts drops to 5% with ECC compared to 75% without it. This stark contrast highlights the effectiveness of ECC in securing user credentials and authentication tokens during transmission, making the HealthAuth system resilient against potential attacks. The implementation of digital signatures further enhances the integrity and authenticity of messages exchanged between users and the authentication server, ensuring that malicious actors cannot tamper with the data.

5 CONCLUSIONS

The HealthAuth system is an essential breakthrough on secure authentication to the healthcare applications combining S-CNN and RNN architectures with ECC. The results indicate that the joint method not only improves user authentication accuracy and reliability by utilizing multi-modal data analysis, but also establishes more secure protection for transmission of sensitive information. The system, which performed at 96.0% accuracy takes in all biometric and behavioral traits we identified that are unique to healthcare settings. Also, purpose of giving proper security through keyless signatures is justified with the sizeable reduction in unauthorized access attempts (from 75% without ECC to only about 5% with ECC) showing how any approach-based security enhancement will be highly resistant against various known attacks. So, users are essentially trading a tiny bit of time for much higher security—and they seem to think that it's well within an acceptable amount. Finally, the HealthAuth architecture provides potential substantially more secure and efficient authentication mechanisms to meet immediate challenges of the health care market which points to future research avenues needed in a direction that may help future enhanced systems using other features data types and specification or machine learning algorithms.

REFERENCES

Servati, M. R., & Safkhani, M. (2023). ECCbAS: An ECC based authentication scheme for healthcare IoT systems. *Pervasive and Mobile Computing*, *90*, 101753.

Ghaffar, Z., Kuo, W. C., Mahmood, K., Tariq, T., Bashir, A. K., & Omar, M. (2024). A Machine Learning Attack Resilient and Low-Latency Authentication Scheme for AI-Driven Patient Health Monitoring System. *IEEE Communications Standards Magazine*, *8*(3), 36-42.

Mahajan, H. B., & Junnarkar, A. A. (2023). Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimedia Tools and Applications*, *82*(28), 44335-44358.

Balakrishnan, D., Rajkumar, T. D., Dhanasekaran, S., & Murugan, B. S. (2024). Secure and energy-efficient data transmission framework for IoT-based healthcare applications using EMCQLR and EKECC. *Cluster Computing*, *27*(3), 2999-3016.

Corthis, P. B., Ramesh, G. P., García-Torres, M., & Ruíz, R. (2024). Effective Identification and Authentication of Healthcare IoT Using Fog Computing with Hybrid Cryptographic Algorithm. *Symmetry*, *16*(6), 726.

Patnaik, A., & Prasad, K. K. (2023). Secure Authentication and Data Transmission for Patients Healthcare Data in Internet of Medical Things. *International Journal of Mathematical, Engineering and Management Sciences*, *8*(5), 1006.

Sheik, S. A., & Durai, S. (2024). Cryptography with optimal deep learning-based authentication scheme for preserving anonymity in telecare medical information system. *Multimedia Tools and Applications*, 1-20.

Chaudhary, D., Kumar, U., & Saleem, K. (2023). A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ecc cryptography. *IEEE Access*.

Sharma, S., Tripathi, S., Bhatt, K. K., & Chhimwal, N. (2024). An Efficient and Secure Authentication Protocol with Deep Learning Based Key Generation toward Securing Healthcare Data in IoT. *Cybernetics and Systems*, *55*(4), 848-871.

Gupta, D. S., Mazumdar, N., Nag, A., & Singh, J. P. (2023). Secure data authentication and access control protocol for industrial healthcare system. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 4853-4864.