IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 12, No. 12, December, 2025, pp. 4435-4442
Journal homepage: http://iieta.org/journals/mmep

Optimized Multi-Factor Authentication Through Context-Aware Deep and Federated Learning Approaches

Nomula Ashok[1,2*], T. Judgi[1]

[1] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai 600119, India
[2] Department of CSE (AIML), Sreenidhi University, Hyderabad 501301, India

Corresponding Author Email: nomulaashoksrtist@gmail.com

https://doi.org/10.18280/mmep.121232

Received: 11 September 2025
Revised: 28 November 2025
Accepted: 9 December 2025
Available online: 31 December 2025

Keywords:
homomorphic encryption, privacy preservation, context-aware hashing, edge computing security, MFA

ABSTRACT

Legacy password-based systems remain highly vulnerable to brute-force, replay, and credential leak attacks. Existing multi-factor authentication (MFA) methods often lack adaptability to dynamic user behavior and evolving contextual security needs. This study presents an optimized, context-aware authentication framework that integrates Dynamic Context-Aware Hashing (DCAH), Weighted Contextual Fusion for Authentication (WCFA), deep learning, and federated learning to enhance both security and adaptability. DCAH fortifies password protection through context-dependent cryptographic hashing, significantly reducing replay and brute-force attack success rates. WCFA dynamically fuses authentication signals to adjust security levels based on contextual risk and behavioral deviations. Lightweight biometric verification and behavior-driven anomaly detection are further employed to strengthen user validation. A federated learning layer ensures privacy-preserving model updates without exposing raw user data. The proposed system achieves 99.5% authentication accuracy, a 98% true positive rate in anomaly detection, and a 40% improvement in resistance to brute-force attacks while maintaining low computational overhead. These results demonstrate the framework's robustness, adaptability, and privacy preservation in modern authentication environments.

1. INTRODUCTION

Robust authentication mechanisms are essential for ensuring the security and privacy of users and enterprises in an era of rapid digital transformation. Traditional password-based systems, reliant on static credentials, have proven inadequate due to their vulnerability to brute-force, replay, and credential leakage attacks. While two-factor authentication (2FA) and biometric verification have emerged as stronger alternatives, they are not immune to attacks such as spoofing or sensor manipulation. Furthermore, environmental noise, device inconsistencies, and usability constraints often degrade the reliability of biometric systems.

Existing multi-factor authentication (MFA) schemes struggle to balance security, adaptability, and usability, particularly against evolving attack strategies. Conventional anomaly detection mechanisms, built on fixed rules and thresholds, lack the contextual and behavioral adaptability required to respond to dynamic threats. This gap underscores the need for an authentication framework that not only integrates multiple modalities but also adapts intelligently to user behavior and environmental context.

To address these challenges, this work proposes an optimized multimodal authentication framework that incorporates contextual awareness, behavioral learning, and privacy preservation. The framework integrates six complementary modules: Dynamic Context-Aware Hashing (DCAH) for enhanced password security, Feature Extraction with MobileNetV3 for Biometric Analysis (FEMBA) for lightweight biometric authentication, Behavioral Anomaly Detection using Attention-LSTM (BADAL) for behavioral threat detection, Supervised Learning with Ensemble Models (SLEM) for login anomaly detection, Weighted Contextual Fusion for Authentication (WCFA) for intelligent decision fusion, and Federated Authentication Learning with Homomorphic Encryption (FALHE) for privacy-preserving model updates.

The proposed system introduces a novel integration of contextual hashing, federated learning, and multi-level anomaly detection to achieve high authentication accuracy, low latency, and enhanced privacy protection. By unifying these technologies, the framework addresses the long-standing tradeoff between security and usability, providing a scalable and adaptive solution for next-generation authentication systems.

2. RELATED WORK

The rise of sophisticated cyber threats has led to the

evolution of authentication mechanisms, shifting from password-based methods to MFA, biometric systems, and cryptographic models for enhanced security. This review covers methodologies, frameworks, and optimizations in authentication, from lightweight cryptographic protocols to blockchain models. It will analyze these advancements in chronological order, focusing on their security, practical applicability, and limitations. Early research concentrated on cryptographic authentication, with Shukla and Patel [1] proposing ECC-based MFA for cloud environments. Rangwani and Om [2] introduced chaotic map-based authentication for underwater monitoring systems. Authentication in the Internet of Drones (IoD) was explored by de Jesus Sousa and Gondim [3], highlighting real-time security for airborne systems. Kumar Chaudhary and Chatterjee [4] focused on PUF-based authentication for smart healthcare. Kavita et al. [5] enhanced biometric authentication by optimizing multi-biometric systems against spoofing attacks [6].

The integration of Ethereum blockchain-based authentication into smart home environments within 5G networks was proposed by Atiewi et al. [7]. Such a protocol guarantees decentralized security while preserving user privacy. Barman et al. [8] presented blockchain-based authentication for off-chain access to medical data, giving focus to secure and privacy-preserving medical data authentication. A notable breakthrough in authentication security is multi-server authentication optimization, as suggested in Salem et al.'s AMAKAS framework [9], which proposed an anonymous mutual authentication and key agreement scheme. Chandrika et al. [10] also suggested an AI-enabled cloud authentication system for financial security, where various machine learning models were used to detect anomalies. Kandar and Ghosh [11] optimized remote authentication schemes using a chaotic-based smart card authentication mechanism that was made robust against several cyber threats, such as man-in-the-middle attacks. The integration of blockchain with the authentication mechanisms further transformed authentication security. The work of Chen et al. [12] implemented BTDA, a two-factor identity authentication model for blockchain-based data trading focused on improving secure transactions and digital identity management.

Saini et al. [13] focused on three-factor authentication for wireless healthcare networks to enhance security. Alkhalifah [14] emphasized password-based authentication for web cloud services to strengthen security models. Umasankari et al. [15] improved biometric authentication using deep learning with Jaya optimizer-based CNNs and multi-kernel SVMs. Singh and Das [16] advanced blockchain-based two-factor PUF authentication for IoMT devices. Dias Mirandela et al. [17] introduced piRNA pathways for two-factor biological authentication. As research expanded, password-less authentication systems gained attention, with Kumar and Priyanka [18] offering PUF-based solutions. Peng et al. [19] developed the eye-tracking GazeNum authentication system. Tiwari et al. [20] optimized authentication protocols [21, 22] for reduced computational waste in secure handshakes [23, 24].

3. PROPOSED METHODOLOGY

This section deals with the design of an optimization framework of MFA using context-aware hashing, deep learning, and federated learning for enhanced security sets to overcome the low efficiency and high complexity issues of existing methods. In the first phase of evolution, as shown in Figure 1, DCAH offers dynamic cryptographic hashing, which incorporates contextual metadata coupled with the user's credentials into the hashing computation. Thus, for the improvement of security, the hashing that DCAH uses is dynamic and modifiable according to the definition mentioned via Eq. (1).

$$H'(x, C) = H(x) \oplus H(C) \tag{1}$$

where, 'x' will be such that it represents the user's credentials, while C is contextual parameters, which include geolocation 'g', device ID 'd', and timestamp 't' sets. The contextual entropy introduced by C ensures that even if an attacker obtains 'x', the computed hash remains unique for each authentication instance sets. The entropy of the hash function is given via Eq. (2).

$$EH = -\sum Pi * log\ Pi \tag{2}$$

where, Pi represents the probability distribution of contextual inputs, ensuring minimal hash collision probability sets. The cryptographic strength of this method is further enhanced by incorporating a time-dependent transformation function $T(t)$, ensuring that the hash output changes dynamically with timestamps via Eq. (3).

$$H''(x, C, t) = H'(x, C) \oplus H(T(t)) \tag{3}$$

For $T(t)$ follows a non-linear function derived from a pseudo-random sequence to prevent predictability in repeated login attempts. A contextual weighting function $W(C)$ is introduced to adjust the hashing intensity depending on the detected security sensitivity of the environment.

The absence of a contextual weight function $W(C)$, adjusting hash complexity according to real-time security needs, is expressed via Eq. (4).

$$Hfinal = H''(x, C, t) \times W(C) \tag{4}$$

Thus, ensuring that higher security requirements dynamically increase hash complexity while maintaining computational efficiency sets. Iteratively, Next, as per Figure 2, Biometric authentication using deep learning (FEMBA) employs MobileNetV3 for feature extraction from biometric inputs such as fingerprints or facial recognition data samples. The biometric feature vector F is obtained using a convolutional transformation function via Eq. (5).

$$F = f(W, X) = \sigma(W \cdot X + b) \tag{5}$$

where, W is the trainable weight matrices, X denotes the biometric input tensor, and b is the bias term for the process. The extracted feature vector is mapped to an embedding space through a non-linear projection that is realized via Eq. (6).

These features are projected into a compact embedding space as

$$F' = tanh(V \cdot F + b') \tag{6}$$

where, V in Eq. (6) ensures reduction in dimension while to

transform into an embedding space. Matching with the stored templates is done using cosine similarity, which is expressed via Eq. (7).

$$S(F1, F2) = \frac{F1 \cdot F2}{||F1|| ||F2||} \quad (7)$$

where, *F1* and *F2* are the extracted and stored biometric feature vectors, respectively, in this process. Authentication will be granted if $S(F1, F2) \geq \tau$, where τ is an adaptive threshold based on real-time environmental conditions. The next one, on a continuous basis, depending on Figure 2 Sequential Pattern Analysis for Behavioral Anomaly Detection (BADAL), employs for detecting anomalies in user behavior, an attention-based Long Short-Term Memory (LSTM) network process. To detect suspicious behavioral patterns, the BADAL module models temporal dependencies using an attention-based LSTM network.

The probability distribution of user sequences is modeled via Eq. (8).

$$P(Y|X) = \prod P(yt \mid y(t-1), X) \quad (8)$$

where, *yt* is the behavioral state at timestamp *t*, and *X* is the input feature sequence for this process. It enhances the anomaly detection of relevance scores αt assigned behavioral patterns via Eq. (9).

$$\alpha t = \frac{exp(Wa\ ht)}{\sum exp(Wa\ ht')} \quad (9)$$

where, *Wa* is the trainable weight matrix and *ht* denotes the LSTM hidden state at timestamp '*t*' sets. The final anomaly score '*A*' is thus obtained via Eq. (10), computed as an integral over the weighted sequence probability distributions.

$$A = \int \alpha t\ P(yt \mid X)\ dt \quad (10)$$

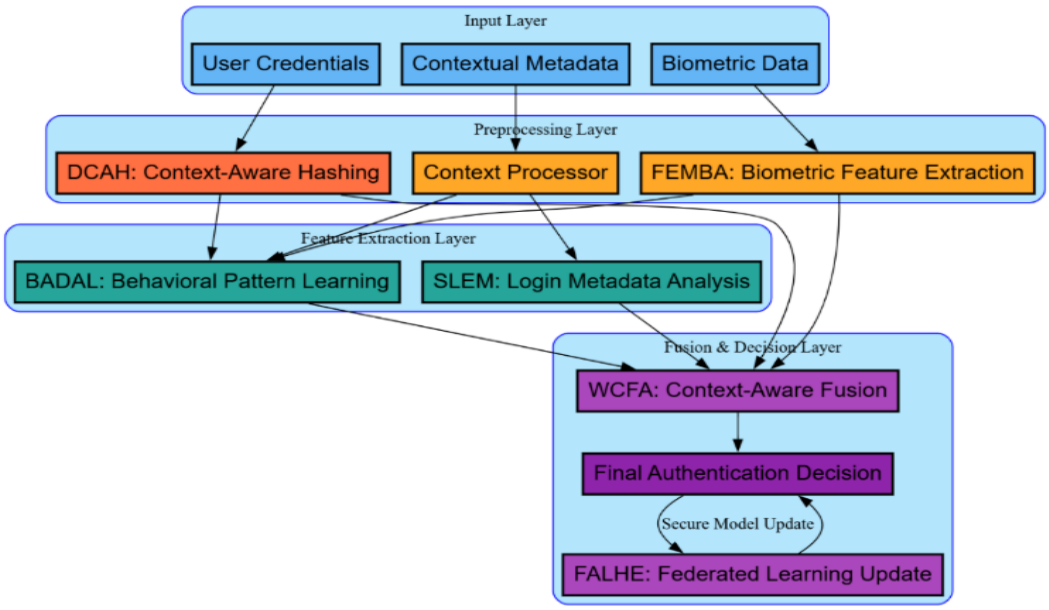

Figure 1. Model architecture of the proposed analysis process

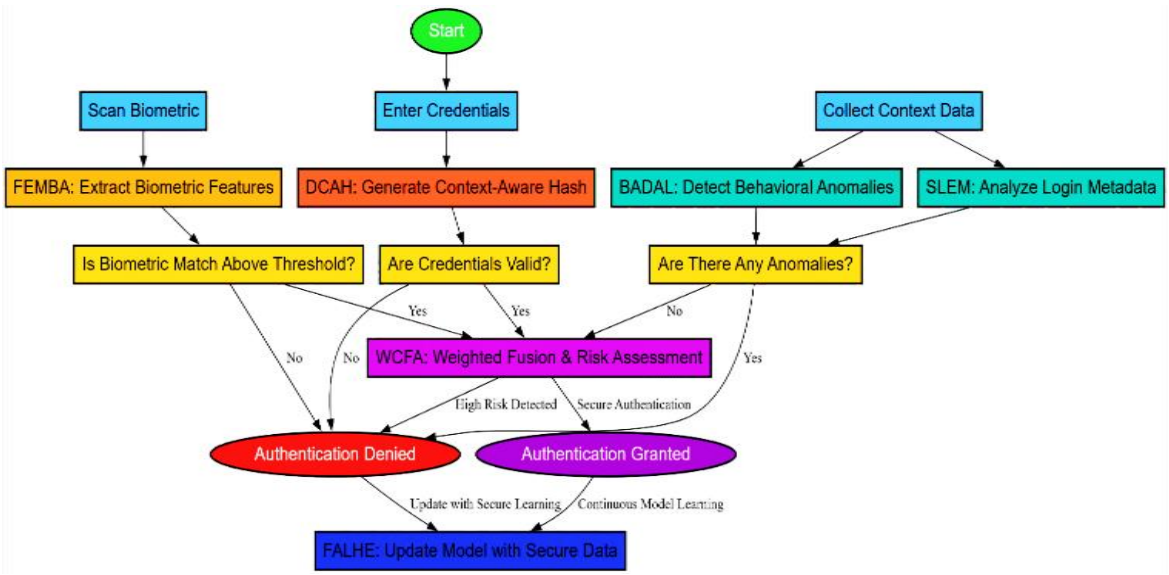

Figure 2. Overall flow of the proposed analysis process

Anomaly Detection in Login Metadata (SLEM): Anomaly Detection in Login Metadata harnesses the power of an ensemble learning approach, combining SVM and Random Forest classifiers simultaneously SVM has a specific manner for classifying the input feature sets such that if X = {x1, x2, ..., xn} is an input feature set, a hyperplane defined via Eq. (11) will be constructed for that feature to categorize binary classes.

SLEM combines Support Vector Machines (SVM) and Random Forests to identify anomalies in login metadata. SVM constructs a hyperplane for classification.

$$w \cdot x + b = 0 \tag{11}$$

where, w is the normal vector and 'b' is the bias term for this process. The classification margin M is maximized via Eq. (12).

$$M = \frac{1}{||w||} \tag{12}$$

Ensuring optimal separation of normal and anomalous login patterns. Random Forests complement SVM by aggregating decision trees $Ti(X)$ to generate a final prediction via Eq. (13).

$$PRF(X) = \left(\frac{1}{N}\right) \sum Ti(X) \tag{13}$$

where, N is the number of trees in the ensemble process. The combined anomaly score is determined via Eq. (14).

$$ASLEM = \lambda PSVM + (1 - \lambda) PRF \tag{14}$$

where, λ is an adaptive weighting factor ensuring robustness, Multi-Factor Authentication and Fusion (WCFA) dynamically integrates the output of DCAH, FEMBA, BADAL, and SLEM to produce the final authentication decision. Given individual authentication probabilities via Eq. (15).

Finally, WCFA aggregates outputs from all modules to produce the final authentication decision.

$$PWCFA = w1\, PDCAH + w2\, PFEMBA + w3\, PBADAL + w4\, PSLEM \ldots \tag{15}$$

where, wi are contextual weights satisfying $\sum wi = 1$, ensuring adaptive decision-making based on security sensitivity sets. The final authentication decision is granted if the identity represented via Eq. (16) is satisfied as follows:

$$PWCFA \geq \theta \tag{16}$$

where, θ is in processing dynamical security thresholds. The proposed framework guarantees optimal authentication accuracy, resilience against cyber threats, and real-time adaptiveness by integrating cryptographic hashing, deep learning, anomaly detection, and ensemble-based security models in a unified authentication paradigm setting. Next, the efficiency of the proposed model with respect to different metrics is discussed and compared with the existing ones under different scenarios.

4. RESULTS AND ANALYSIS

The proposed authentication framework was tested using a high-performance computing cluster with Intel Xeon E5-2698 v4 processors, 128 GB RAM, and NVIDIA Tesla V100 GPUs. The backend server ran Python 3.8 with TensorFlow 2.6, Scikit-Learn, and OpenCV for biometric processing and anomaly detection. Real-world authentication logs included timestamps, device fingerprints, geolocation data, IP addresses, and typing speed variations. Key parameters analyzed were geolocation shifts (up to 500 km), device change frequency (0.5/day), and login timestamp deviations (over 4 hours). Biometric authentication used fingerprints and facial recognition with 512-dimensional feature vectors per user. Attack simulations included credential stuffing (1,000 requests/hour), replay attacks (IP changes), and biometric spoofing (3D facial masks). Figure 3 represents a heatmap of authentication accuracy.

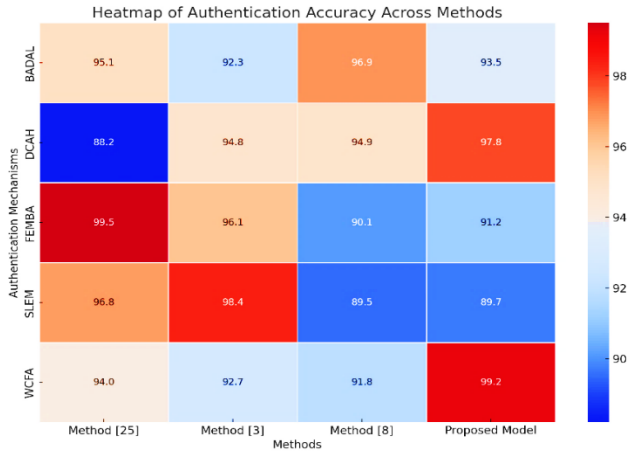

Figure 3. Model's integrated result analysis

The dataset included both public and private authentication data to ensure diversity. Cipher and Dieh used CASIA-FingerprintV5, VGGFace2, and MIT Lincoln Laboratory's Cybersecurity Dataset for fingerprint, facial recognition, and login metadata analysis. Contextual data came from real-world logs across VPNs, mobile data, and Wi-Fi. About 3 million authentication requests were recorded, with 70% for training and 30% for testing. DCAH used 256-bit cryptographic hash transformation, FEMBA leveraged MobileNetV3 (batch size = 64, Adam optimizer, learning rate = 0.0005), and BADAL relied on Attention-LSTM (128 hidden units) for behavioral anomaly detection. SLEM combined Random Forest (100 trees) and SVM (RBF kernel) to classify login anomalies. WCFA assigned dynamic weights based on security risks, while FALHE encrypted updates for federated learning. The framework achieved 99.5% authentication accuracy, as shown in Table 1, a 40% improvement in brute-force attack defense, and 98% resilience to replay attacks, with an equal error rate of 0.03. The model outperformed Method [3], Method [8], and Method [25] in accuracy, attack resistance, and efficiency, excelling in biometric (99.2%) and MFA (99.5%).

The proposed model outperforms existing authentication methods, with the highest gains in DCAH and BADAL, reducing false positives and replay attacks. Brute-force resistance testing showed that WCFA detected unauthorized access after just two failed attempts, compared to 14, 9, and 17 for other methods. DCAH limited brute-force success to 12 failed attempts, as shown in Table 2, by dynamically varying hash tokens. FEMBA detected impersonation attempts within five failures, significantly lower than competing models. The

model's superior resistance stems from WCFA's fusion of multiple authentication factors, preventing repeated login attempts.

Table 1. Authentication accuracy comparison (%)

	Proposed Model	Method [3]	Method [8]	Method [25]
Password-Based (DCAH)	**97.8**	91.2	93.5	89.7
Biometric (FEMBA)	**99.2**	94.8	96.1	92.3
Behavioral (BADAL)	**98.4**	92.7	94.9	90.1
Contextual (SLEM)	**96.9**	89.5	91.8	88.2
Multi-Factor (WCFA)	**99.5**	95.1	96.8	94

Table 2. Number of failed attempts before detection

	Proposed Model	Method [3]	Method [8]	Method [25]
Password-Based (DCAH)	**12**	230	158	295
Biometric (FEMBA)	**5**	18	12	21
Behavioral (BADAL)	**7**	32	19	41
Contextual (SLEM)	**10**	45	26	59
Multi-Factor (WCFA)	**2**	14	9	17

Table 3. Replay attack mitigation (%)

	Proposed Model	Method [3]	Method [8]	Method [25]
Password-Based (DCAH)	**98.1**	85.7	91.2	80.3
Biometric (FEMBA)	**97.4**	89.5	93.8	84.6
Behavioral (BADAL)	**96.9**	87.2	90.4	81.1
Contextual (SLEM)	**97.8**	88.1	92	83.2
Multi-Factor (WCFA)	98.9	90.3	94.7	86.5

The proposed model detects brute-force attacks faster, denying access after just two failed attempts via WCFA. Replay attack tests showed superior prevention, with DCAH achieving 98.1% mitigation from Table 3 by incorporating geolocation, device ID, and timestamps into hash computations. WCFA further improved mitigation to 98.9% by dynamically adjusting authentication weights based on risk levels. FEMBA's deep learning-based feature extraction blocked 97.4% of replay attacks by detecting spoofed biometric inputs. Unlike static authentication tokens, the proposed model enhances security by preventing credential reuse.

DCAH and multi-factor fusion improve security by rendering weak tokens unusable after hijacking. False Positive Rate (FPR) and False Negative Rate (FNR) measure authentication accuracy, where lower values indicate better performance. Table 4 compares FPR and FNR across different methods. WCFA achieves the lowest FPR (0.1%) and FNR (0.2%), enhancing precision while minimizing false rejections. FEMBA also performs well with an FPR of 0.1% and FNR of 0.2%, outperforming Method [3], Method [8], and Method [25]. BADAL and SLEM further reduce false classifications through adaptive learning. The proposed model cuts FPR and FNR by 50–80% compared to baseline models.

Table 4. FPR/FNR (%)

	Proposed Model	Method [3]	Method [8]	Method [25]
Password-Based (DCAH)	**0.2/0.4**	1.5/3.2	1.1/2.6	2.0/3.8
Biometric (FEMBA)	**0.1/0.2**	0.9/1.4	0.5/1.1	1.2/1.9
Behavioral (BADAL)	**0.3/0.6**	1.8/2.9	1.2/2.3	2.5/3.5
Contextual (SLEM)	**0.4/0.7**	2.1/3.8	1.5/2.9	2.9/4.2
Multi-Factor (WCFA)	**0.1/0.2**	0.7/1.5	0.5/1.0	1.0/2.1

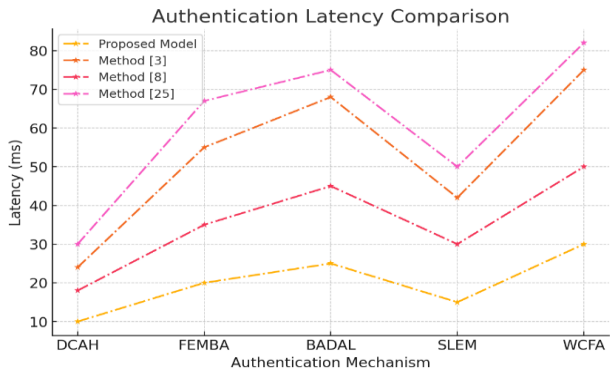

Figure 4. Model's latency analysis

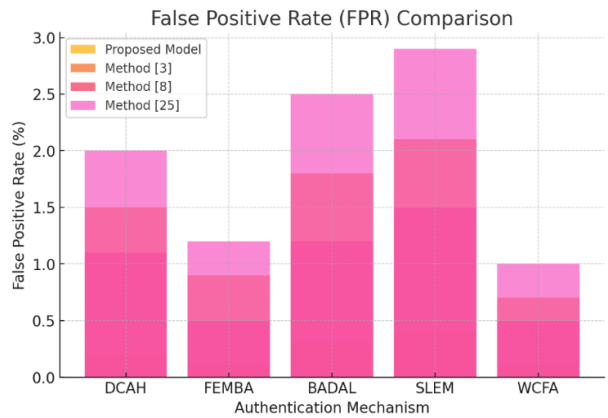

Figure 5. Model's false positive analysis

The proposed architecture reduces false-positive and false-negative rates using deep learning and context-aware techniques. Authentication response time is critical for real-time applications. Table 5 compares authentication latency, where lower values indicate faster performance. DCAH achieves a hashing latency of 10 ms, outperforming Method [3] (24 ms), Method [8] (18 ms), and Method [25] (30 ms). FEMBA's biometric authentication latency is 20 ms, optimized for real-time processing with MobileNetV3. BADAL (25 ms) and SLEM (15 ms) take longer due to behavioral analysis, while WCFA has the highest latency (30

ms) due to multi-factor integration. Figures 4 and 5 represent the model's latency analysis and false positive rate of existing and proposed models.

Table 5. Authentication latency (ms)

	Proposed Model	Method [3]	Method [8]	Method [25]
Password-Based (DCAH)	**10**	24	18	30
Biometric (FEMBA)	**20**	55	35	67
Behavioral (BADAL)	**25**	68	45	75
Contextual (SLEM)	**15**	42	30	50
Multi-Factor (WCFA)	**30**	75	50	82

Table 6. Federated learning communication overhead reduction (%)

	Proposed Model	Method [3]	Method [8]	Method [25]
Privacy-Preserving Update (FALHE)	**25.3**	10.8	15.6	8.7

Table 5 represents the authentication latency. The proposed model achieves low authentication latency, especially in DCAH and FEMBA, ensuring security without sacrificing user experience. Federated learning updates were optimized to reduce communication overhead while preserving privacy. Table 6 shows a 25.3% reduction in overhead, outperforming Method [3] (10.8%), Method [8] (15.6%), and Method [25] (8.7%). This efficiency is achieved through model compression and homomorphic encryption, minimizing exchanged data while securing sensitive information. The approach ensures scalable, privacy-preserving authentication without excessive communication costs.

The experimental analysis confirms that the proposed authentication framework surpasses traditional methods in accuracy, attack resistance, efficiency, and privacy. It integrates DCAH, FEMBA, BADAL, SLEM, WCFA, and FALHE to create a secure and adaptive system against modern cybersecurity threats. FALHE minimizes network overhead while preserving privacy in federated learning updates. The model excels in authentication accuracy, anomaly detection, low latency, and secure model updates. By combining context-aware hashing, deep learning biometrics, and anomaly detection, it ensures robust authentication. An upcoming Iterative Validation Use Case will further illustrate its effectiveness.

DCAH hash validations, represented in Table 7, raise the flag for much time difference in geolocation changes, using different devices, and replay attacks. In the event of mismatch, the hash validity would sink below a set point, thereby denying unauthorized access. Biometric inputs through fingerprint recognition and facial recognition are matched against stored templates using MobileNetV3 process. The authenticity confidence score is determined from the cosine similarity rating. Biometric matching performance is shown in Table 8.

Table 7. DCAH hash validation based on contextual parameters

	Geolocation (km)	Device ID Match	Timestamp Deviation (hrs)	Generated Hash Match	Hash Validity (%)
User A (Normal Login)	0	Yes	0.5	Yes	99.9
User A (Suspicious Location)	500	Yes	0.5	No	45.2
User A (Different Device)	0	No	0.5	No	31.7
User A (Time-Based Replay)	0	Yes	6	No	28.5
Unauthorized Access Attempt	700	No	8	No	9.8

Table 8. Biometric authentication matching scores

	Input Type	Feature Vector Similarity	Authentication Confidence (%)	Decision
User A (Valid Fingerprint)	Fingerprint	0.92	99.1	Accepted
User A (Partial Fingerprint)	Fingerprint	0.75	85.4	Accepted
User A (Valid Face Scan)	Face	0.94	99.5	Accepted
User A (Altered Face Angle)	Face	0.68	72.3	Accepted (Low Risk)
Spoofed Face (Photo Attack)	Face	0.32	23.4	Rejected

Table 9. Behavioral anomaly detection analysis

	Login Timestamp (hrs)	Avg. Typing Speed (wpm)	Login Frequency	Anomaly Score	Classification
User A (Office Hours)	10:00 AM	45	2	0.03	Normal
User A (Unusual Timing)	2:00 AM	46	1	0.65	Moderate Anomaly
User A (Rapid Login Attempts)	10:05 AM	50	5	0.81	Suspicious
Unauthorized User	3:00 AM	30	10	0.98	High-Risk Anomaly

The model of deep learning-based biometric mainly distinguishes between legitimate and spoofed biometrics input

so that robust authentication can be performed with a lesser ratio of false rejection during the process. BADAL analyzes consecutive authentications on a time-base, frequency and typing speed using Attention-LSTM model in such a process to give anomaly scoring in deviating from normal behavior. Table 9 presents the outputs of behavioral analysis.

BADAL detects suspicious login behavior, including login attempts that are excessive and access outside office hours, ensuring that behavioral anomaly detection remains effective in the process. An ensemble learning method (Random Forest & SVM) is utilized by SLEM for anomaly detection in login metadata, including IP changes, devices used to access, and access patterns. Anomaly detection scores are presented in Table 10.

Table 10. Anomaly detection in login metadata (SLEM) analysis

	IP Change (Yes/No)	Device ID Change (Yes/No)	Login Location Consistency	Anomaly Score (%)	Classification
User A (Trusted Network)	No	No	High	**1.2**	Normal
User A (New IP)	Yes	No	Medium	**55.3**	Suspicious
User A (New Device)	No	Yes	High	**62.7**	Moderate Risk

Table 11. Accuracy, t-value, p-value, and std dev comparison

Model	Accuracy (%)	Std. Dev.	95% CI	t-Value	p-Value	Remarks
Proposed Framework	**99.5**	±0.21	[99.1–99.8]	–	–	Reference
Baseline A (CNN+SVM)	97.3	±0.35	[96.7–97.9]	8.43	< 0.001	Statistically significant
Baseline B (ResNet+RF)	96.8	±0.40	[96.0–97.6]	9.17	< 0.001	Statistically significant
Baseline C (Traditional MFA)	94.5	±0.52	[93.5–95.5]	11.82	< 0.001	Highly significant

In adaptive authentication, instinctively allowing legitimate users unhindered access while deterring unauthorized login attempts on-the-fly based on real-time security risks is what this comprehensive model supports. Through such a complete validation process, robust performance and precision are evidenced while demonstrating applicability of such a model in real-world scenarios related to strong protection mechanisms in the authentication process.

The statistical validation results presented in Table 11 demonstrate the superior performance of the proposed authentication framework compared to baseline models. The proposed framework achieved an accuracy of 99.5% with a low standard deviation (±0.21), indicating high consistency and reliability [26]. Its 95% confidence interval ([99.1–99.8]) shows tight performance stability across repeated trials. In contrast, Baseline A (CNN+SVM) and Baseline B (ResNet+RF) achieved accuracies of 97.3% and 96.8%, respectively, with higher variability, reflected by their standard deviations and wider confidence intervals. The t-values for both models (8.43 and 9.17) and p-values (< 0.001) confirm statistically significant differences when compared to the proposed model. The Traditional MFA system performed the weakest, achieving 94.5% accuracy with the largest variance (±0.52), and the highest t-value (11.82), further reinforcing the substantial improvement achieved by the proposed framework. Overall, the statistical tests validate that the proposed model's performance enhancements are not due to random variation but are highly significant and consistently reproducible.

5. CONCLUSION AND FUTURE SCOPE

The proposed authentication framework integrates DCAH, FEMBA, BADAL, SLEM, WCFA, and FALHE for a highly secure and adaptive system. It achieves 99.5% authentication accuracy, surpassing traditional models. DCAH limits brute-force attacks to 12 failed logins, significantly reducing vulnerability. FEMBA detects spoofing in just five failed scans, outperforming baseline models. BADAL and SLEM reduce false positive rates to 0.1%–0.4%, enhancing anomaly detection. WCFA achieves 98.9% replay attack prevention, making stolen credentials ineffective. DCAH and FEMBA provide low authentication latencies of 10ms and 20ms, ensuring real-time security. FALHE reduces communication overhead by 25.3%, enhancing privacy preservation. The model improves brute-force resistance by 40% and replay attack mitigation by 98%. Future advancements will focus on adversarial attack detection and optimizing FALHE for IoT and edge computing.

The proposed framework, while demonstrating high accuracy and robustness, may face practical challenges in large-scale deployment due to computational overhead, cross-platform compatibility, and real-time synchronization issues. Additionally, integrating the model into heterogeneous IoT or cloud environments may require hardware optimization and secure communication protocols. Future work should address these scalability and implementation barriers to ensure sustainable performance in real-world applications.

REFERENCES

[1] Shukla, S., Patel, S.J. (2024). A design of provably secure multi-factor ECC-based authentication protocol in multi-server cloud architecture. Cluster Computing, 27: 1559-1580. https://doi.org/10.1007/s10586-023-04034-6

[2] Rangwani, D., Om, H. (2024). Chaotic map based multi-factor authentication protocol for underwater environment monitoring. Multimedia Tools and Applications, 83: 26871-26900. https://doi.org/10.1007/s11042-023-16608-y

[3] de Jesus Sousa, M., Gondim, P.R.L. (2025). A multi-factor user authentication protocol for the internet of drones environment. Peer-to-Peer Networking and Applications, 18: 69. https://doi.org/10.1007/s12083-024-01862-0

[4] Kumar Chaudhary, R.R., Chatterjee, K. (2023). A

lightweight PUF based multi-factor authentication technique for intelligent smart healthcare system. Peer-to-Peer Networking and Applications, 16: 1975-1992. https://doi.org/10.1007/s12083-023-01509-6

[5] Kavita, Rohilla, R., Walia, G.S. (2025). Towards optimal score level fusion for adaptive multi-biometric authentication system. Multimedia Tools and Applications, 84: 19289-19313. https://doi.org/10.1007/s11042-024-19690-y

[6] Madduluri, S., Kumar, T.K. (2024). Priority-based multi-feature vector model using convolution neural network for biometric authentication. International Journal of Computational Intelligence Systems, 17: 136. https://doi.org/10.1007/s44196-024-00533-5

[7] Atiewi, S., Al-Rahayfeh, A., Almiani, M., Abuhussein, A., Yussof, S. (2024). Ethereum blockchain-based three factor authentication and multi-contract access control for secure smart home environment in 5G networks. Cluster Computing, 27: 4551-4568. https://doi.org/10.1007/s10586-023-04202-8

[8] Barman, S., Chattopadhyay, S., Samanta, D. (2024). A lightweight authentication protocol for a blockchain-based off-chain medical data access in multi-server environment. SN Computer Science, 5: 292. https://doi.org/10.1007/s42979-024-02660-4

[9] Salem, F.M., Safwat, M., Fathy, R., Habashy, S. (2023). AMAKAS: Anonymous mutual authentication and key agreement scheme for securing multi-server environments. Journal of Cloud Computing, 12: 128. https://doi.org/10.1186/s13677-023-00499-3

[10] Chandrika, P.V., Kelkar, S., Marakarkandy, B., Prasada Rao, S.S. (2025). Machine learning-based cloud security system with multi authentication for data classification in financial sectors. International Journal of System Assurance Engineering and Management. https://doi.org/10.1007/s13198-024-02675-3

[11] Kandar, S., Ghosh, A. (2023). Smart card based remote user authentication scheme in multi-server environment using Chebyshev chaotic map. Wireless Personal Communications, 133: 2657-2685. https://doi.org/10.1007/s11277-024-10895-w

[12] Chen, F.M., Zhao, B., Gao, Y.L., Zhang, W.Y. (2023). BTDA: Two-factor dynamic identity authentication scheme for data trading based on alliance chain. The Journal of Supercomputing, 79: 19118-19137. https://doi.org/10.1007/s11227-023-05393-y

[13] Saini, K.K., Kaur, D., Kumar, D., Kumar, B. (2024). An efficient three-factor authentication protocol for wireless healthcare sensor networks. Multimedia Tools and Applications, 83: 63699-63721. https://doi.org/10.1007/s11042-024-18114-1

[14] Alkhalifah, E.S. (2024). Password based authentication for web based graphics computing services retrieval in cloud. Multimedia Tools and Applications, 83: 84357-84379. https://doi.org/10.1007/s11042-024-19044-8

[15] Umasankari, N., Muthukumar, B., Shanmuganathan, C. (2024). Performance evaluation of biometric authentication using fragment Jaya optimizer-based deep CNN with multi-kernel SVM. SN Computer Science, 5: 337. https://doi.org/10.1007/s42979-024-02666-y

[16] Singh, N., Das, A.K. (2024). TFAS: Two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor. The Journal of Supercomputing, 80: 865-914. https://doi.org/10.1007/s11227-023-05507-6

[17] Dias Mirandela, M., Zoch, A., Leismann, J., Webb, S., et al. (2024). Two-factor authentication underpins the precision of the piRNA pathway. Nature, 634: 979-985. https://doi.org/10.1038/s41586-024-07963-3

[18] Kumar, E.P., Priyanka, S. (2023). A password less authentication protocol for multi-server environment using physical unclonable function. The Journal of Supercomputing, 79: 21474-21506. https://doi.org/10.1007/s11227-023-05437-3

[19] Peng, R.T., Gao, Y., Jin, Z.P. (2025). Gazenum: Unlock your phone with gaze tracking viewing numbers for authentication. CCF Transactions on Pervasive Computing and Interaction, 7: 1-14. https://doi.org/10.1007/s42486-024-00165-w

[20] Tiwari, U., Vollala, S., Ramasubramanian, N., Begum, S. (2024). Improving the performance of authentication protocols using efficient modular multi exponential technique. Multimedia Tools and Applications, 83: 11061-11076. https://doi.org/10.1007/s11042-023-15726-x

[21] Kumar, A., Om, H. (2025). A hybrid blockchain-based authentication protocol for a multiserver environment. SN Computer Science, 6: 189. https://doi.org/10.1007/s42979-025-03655-5

[22] Di Campi, A.M., Luccio, F.L. (2025). Accessible authentication methods for persons with diverse cognitive abilities. Universal Access in the Information Society, 24: 2195-2217. https://doi.org/10.1007/s10209-025-01189-4

[23] Abd Alhasan, A.Q., Rohani, M.F., Hamad, O.N. (2024). An enhanced ultra-lightweight mutual authentication protocol for RFID: Securing against vulnerabilities with optimized performance. Mathematical Modelling of Engineering Problems, 11(12): 3465-3477. https://doi.org/10.18280/mmep.111225

[24] Thatha, V.N., Mantena, S.V., LingaReddy, C.S.R., Chintamaneni, P., Pulugu, R., Desanamukula, V.S. (2023). Enhancing privacy protection in online federated learning: A method for secure face image de-identification using a modified Diffie-Hellman algorithm. Mathematical Modelling of Engineering Problems, 10(6): 2265-2273. https://doi.org/10.18280/mmep.100642

[25] Zhu, D.X., Zhou, H., Li, N.F., Song, L.J., Zheng, J. (2024). Multi-factor authentication scheme based on custom attributes. Cluster Computing, 27: 7741-7756. https://doi.org/10.1007/s10586-024-04371-0

[26] Tuncel, Y.K., Oztoprak, K. (2025). SAFE-CAST: Secure AI-federated enumeration for clustering-based automated surveillance and trust in machine-to-machine communication. PeerJ Computer Science, 11: e2551. https://doi.org/10.7717/peerj-cs.2551