Password Encryption in Cyber Security: Advanced Hybrid Frameworks and Biometric Integration

Dr. Densy John Vadakkan[1], Aurangjeb Khan[2], Neha Patni[3], Sandhya R S[4]
[1] *Senior Assistant Professor, School of Science and Computer Studies, CMR University, Bengaluru*
[2] *Assistant Professor, School of Science and Computer Studies, CMR University, Bengaluru*
[3,4] *Student, Master of Computer Application, School of Science and Computer Studies, CMR University, Bengaluru*

***Abstract*—The rapid growth of digital technologies has increased the need for secure authentication mechanisms to protect sensitive information and digital identities. Traditional password-based systems are vulnerable to attacks such as brute force, phishing, and credential stuffing, making stronger authentication methods essential.**

This paper proposes a Hybrid Adaptive Authentication Framework (HAAF) that integrates Braille-based password transformation, biometric authentication, fuzzy extractor-based key generation, machine learning-driven adaptive cryptography, and blockchain-enabled access control. The framework aims to enhance security, privacy, and resistance to evolving cyber threats. Experimental assessment using simulated datasets reveals that the proposed framework provides improved authentication accuracy and stronger protection against unauthorized access compared with conventional password-based systems.

***Index Terms*—Password Encryption, Cybersecurity, Multi-Factor Authentication, Biometric Authentication, Fuzzy Extractors, Machine Learning, Adaptive Cryptography, Blockchain Security.**

I. INTRODUCTION

The swift growth of cloud computing, mobile applications, and the Internet of Things (IoT) has increased the need for secure access to digital systems. Authentication mechanisms play a vital role in protecting sensitive information by validating user identities before granting access.

Traditional password-based authentication systems are widely used but persistently vulnerable to attacks such as brute-force attacks, phishing, and credential theft. Although techniques such as PBKDF2, bcrypt, and Argon2 improve password security, they cannot adapt to evolving cyber threats. Multi-factor authentication and biometric authentication provide additional security but face challenges related to usability, privacy, and secure storage of sensitive data. Recent developments in machine learning enable adaptive authentication by analysing user behaviour and detecting anomalies, while blockchain technology offers secure and decentralized access control. However, these tactics are often executed independently and fail to deliver a complete security solution.

To address these limitations, this project proposes a Hybrid Adaptive Authentication Framework (HAAF) that integrates password transformation, biometric authentication, cryptographic key generation, machine learning-based adaptive security, and blockchain-enabled access control. The proposed framework aims to enhance security, protect user privacy, and provide a robust authentication mechanism for modern digital environments.

II. LITERATURE REVIEW

With the growing demand for secure digital identity verification and the proliferation of advanced cyber threats, the field of password encryption and authentication has seen significant developments. Unfortunately, with the advent of faster computers and more powerful cracking software that utilizes graphics processing units, such hashing systems have fallen out of grace from the attacks of brute force and dictionary attacks [1][2].

To overcome these challenges, more sophisticated key derivation functions were developed, such as

PBKDF2, bcrypt, and argon2, which add salting and iterative hashing to make the computation more difficult and resistant to attacks [3] [4].

Research shows that the use of MFA can dramatically lower the risk of unauthorized access, since it would need an attacker to break through multiple independent factors [5] [6]. Most traditional MFA systems use both smart cards and one-time password (OTP), which are also vulnerable to attacks like interception of OTPs and stealing the token; and present usability issues. [7].

Biometric characteristics are unique to humans and hard to duplicate, hence they offer more identity assurance than passwords. [8] [9]. Biometric systems, however, have privacy, template security and input variability issues. Because biometric data cannot be altered if it is breached, it is important to secure biometric templates.

A fuzzy extractor is able to reconstruct the same key regardless of small variations in biometric readings, thereby enhancing security and usability [10] [11]. It has been demonstrated that biometric authentication in combination with fuzzy extractors can improve the security level against replay attacks, impersonation and biometric leakage [12]. Further, fuzzy extractors with passwords have been proposed to leverage the password entropy with biometric entropy to generate more robust cryptographic keys and making it harder to launch an offline attack [13].

Based on their user behavior, machine learning models can identify anomalies and dynamically increase the level of authentication according to the risk perceived [14] [15]. The system can, for instance, boost the number of hashing iterations or demand extra biometric verification in case of suspicious activity.

Another area where blockchain technology shows potential is in the authentication security, where the decentralized access control and tamper-resistant record management enhance the security of authentication processes. While centralized authentication systems are subject to single point of failure and insider attacks, blockchain offers a distributed and immutable ledger to securely record the authentication events [16] [17]. Smart contracts can automatically and transparently implement authentication policies, minimizing the potential for unauthorized access. It has been shown recently that blockchain-based biometric authentication systems offer improved privacy, integrity and trust in distributed systems [18].

While these improvements have been made, current systems have some drawbacks, such as computational complexity, isolated systems and scalability issues. Some solutions have concentrated on the technology itself, biometric authentication, adaptive cryptography, or blockchain, but no one has yet developed a well-integrated architecture that integrates these technologies into a single secure framework [19]. Moreover, the lightweight and secure authentication mechanism is an open research problem for resource constrained environments like IoT networks [20].

III. PROPOSED HYBRID ADAPTIVE AUTHENTICATION FRAMEWORK (HAAF)

As cyber threats continue to evolve, traditional authentication mechanisms are no longer sufficient to provide robust security. To address these challenges, this research proposes a Hybrid Adaptive Authentication Framework (HAAF) that integrates password transformation, biometric authentication, fuzzy extractor-based key generation, machine learning-driven adaptive cryptography, and blockchain-enabled access control into a unified framework.

A. DESIGN OBJECTIVES

The HAAF framework aims to provide:

- High Security: Protection against brute-force, phishing, credential stuffing, and replay attacks.
- Privacy Preservation: Secure handling of passwords and biometric data.
- Real-Time Threat Detection: Dynamic adjustment of security measures based on risk levels.
- Scalability: Support for secure and scalable applications.
- Interoperability: Integration with different systems through blockchain technology.

B. ARCHITECTURAL OVERVIEW

HAAF consists of four layers:

1. Input and Preprocessing Layer
2. Transformation and Entropy Enhancement Layer
3. Biometric Fusion and Key Generation Layer
4. Adaptive Cryptography Layer

These layers work together to provide secure and adaptive authentication.

1. INPUT AND PREPROCESSING LAYER

The authentication process begins with a textual password and a biometric sample. The inputs are pre-processed and standardized to improve reliability and authentication accuracy.

2. TRANSFORMATION AND ENTROPY ENHANCEMENT LAYER

To strengthen password security, HAAF employs a Braille-based transformation mechanism that converts passwords into binary sequences, increasing entropy and improving resistance to brute-force and dictionary attacks.

$$P = \{p_1, p_2, p_3, \ldots, p_n\}$$

After transformation:

$$P' = f_{braille}(P)$$

2.1. JUSTIFICATION OF BRAILLE-BASED PASSWORD TRANSFORMATION

The proposed HAAF framework employs a Braille-based password transformation mechanism to enhance password security and increase resistance against conventional cyberattacks. The selection of Braille encoding is motivated by its ability to introduce additional complexity and improve the unpredictability of password representations.

In traditional authentication systems, passwords are represented using standard character encodings such as ASCII, which are fixed and widely known. Since attackers are familiar with these encoding schemes, password databases become more vulnerable to dictionary attacks, brute-force attacks, and pattern-based guessing. In contrast, Braille-based encoding converts each character into a unique binary pattern, creating an additional transformation layer that makes reverse engineering more difficult.

Method	Strength	Weakness
ASCII Encoding	Standard, fast	Predictable, widely attacked
Random Encoding	High randomness	Requires key sharing, less deterministic
Braille Encoding (Proposed)	Structured unpredictable	Slight overhead

Furthermore, the transformation process improves practical password entropy and introduces greater structural randomness. Attackers must not only determine the original password but also identify the transformation scheme used, thereby increasing the computational effort required to compromise the system. This additional level of uncertainty provides stronger protection compared with conventional password encoding methods.

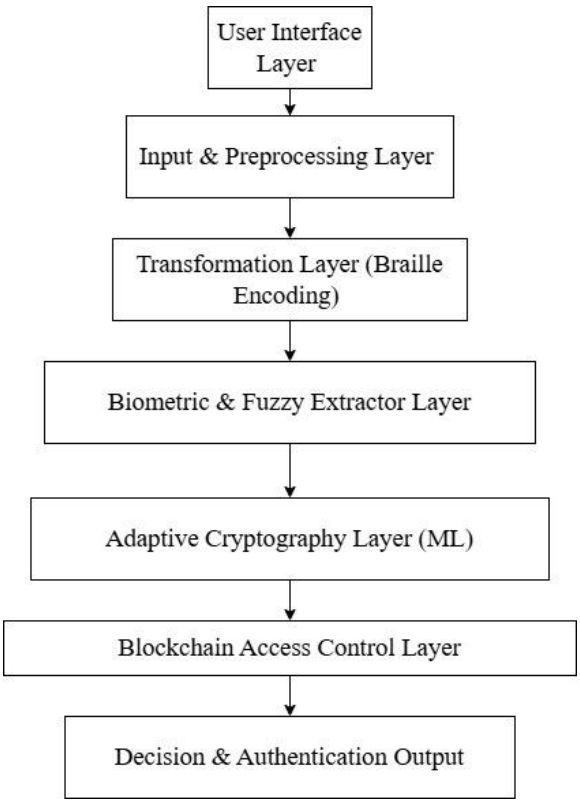

Fig 1: Authentication Workflow Diagram

Therefore, the Braille-based password transformation mechanism serves as an effective approach for enhancing password strength and forms an important component of the proposed Hybrid Adaptive Authentication Framework.

TABLE1: COMPARISON WITH RANDOM ENCODING TECHNIQUES

3. BIOMETRIC FUSION AND KEY GENERATION LAYER

The framework combines biometric authentication with cryptographic key generation through fuzzy extractors. Because biometric data can vary, fuzzy extractors generate consistent cryptographic keys from unreliable inputs.

The fuzzy extractor consists of two functions:

- Gen(b) → Generates a key K and helper data W from biometric input b

- Rep(b', W) → Reproduces the same key K using a similar biometric input b'

$$(K, W) = Gen(b)$$
$$K = Rep(b', W)$$

To make it more secure the system mixes the changed password with the key that comes from your data. The system uses this key along, with the transformed password. This helps to provide a layer of security. The transformed password and biometric key are combined to achieve this.:

$$K_{final} = H(P' \oplus K)$$

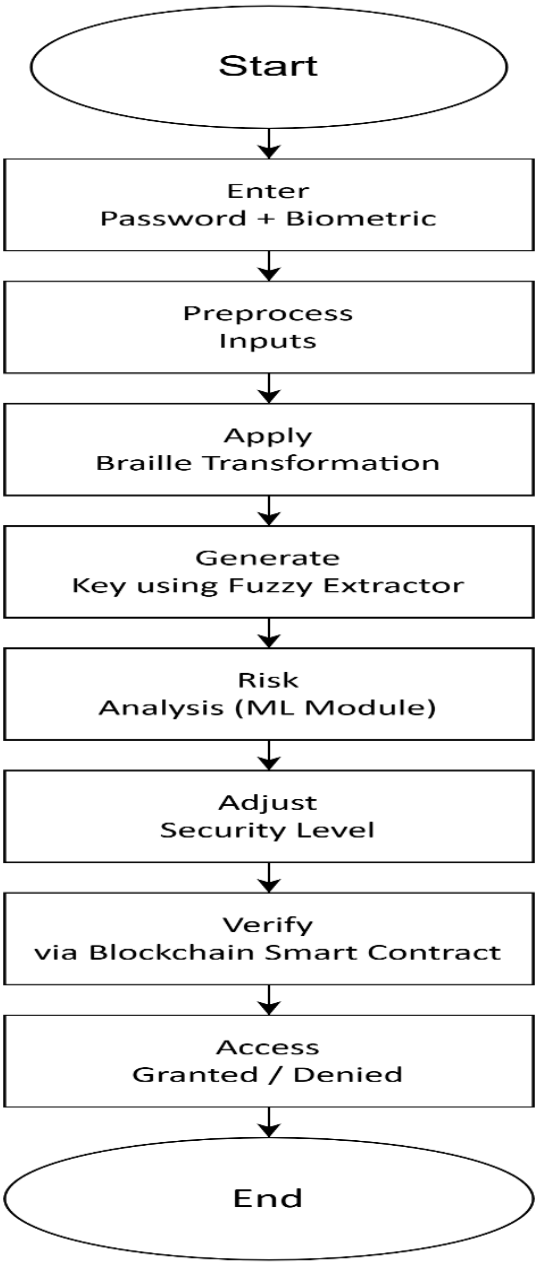

Fig 2: Layered Architecture of HAAF

4.ADAPTIVE CRYPTOGRAPHY LAYER

One of the things that makes HAAF special is that it uses machine learning to make its cryptography better. The HAAF system has a layer that always watches what the users are doing and what is happening in the system. This helps the HAAF system find things that're not normal and things that could be a problem, for the HAAF system.

A machine learning model, such as an anomaly detection or classification algorithm, analyses features including login frequency, IP address and location, device fingerprint, and failed login attempts to detect suspicious activities.

H. AUTHENTICATION WORKFLOW

The complete authentication process in HAAF can be summarized as follows:

1. User enters password and provides biometric input
2. Password is transformed using Braille encoding
3. Biometric data is processed using a fuzzy extractor
4. A hybrid cryptographic key is generated
5. Machine learning module evaluates risk level
6. Encryption parameters are adjusted dynamically
7. Blockchain smart contract verifies access conditions
8. Access is granted or denied based on verification results

I. SECURITY FEATURES OF HAAF

The proposed framework provides several advanced security features:

- Resistance to Brute-Force Attacks: High entropy password transformation and adaptive hashing
- Protection Against Credential Theft: Multi-factor authentication using biometrics
- Privacy Preservation: No storage of raw biometric data
- Adaptive Defence: Real-time response to threats using machine learning
- Tamper-Proof Access Control: Blockchain-based verification

J. PERFORMANCE EVALUATION

The Hybrid Adaptive Authentication Framework is a way to secure digital identities. It uses a combination of password changes, biometric security, machine learning and blockchain to control access. This framework gives us a flexible and safe way to authenticate users. The Hybrid Adaptive

Authentication Framework tackles today's cybersecurity problems. It does this by combining password transformation, with cryptography and adaptive machine learning and blockchain-based access control.

K. EVALUATION METRICS

To assess the performance of the proposed framework, the following key metrics are considered:

- Execution Time (ET): Measures the total time required for authentication, including password processing, biometric verification, and cryptographic operations.
- False Acceptance Rate (FAR): This refers to the probability that an unauthorized user is incorrectly granted access.
- False Rejection Rate (FRR): This denotes the probability that a legitimate user is incorrectly denied access.
- Equal Error Rate (EER): This point refers where FAR equals FRR, which is used as an overall accuracy indicator.
- Security Strength: This indicates resistance to brute-force, dictionary, and replay attacks.
- Throughput: This is the number of authentication requests processed per second.
- Scalability: Refer to the system performance under increasing user load.

L. SIMULATION METHODOLOGY

The performance evaluation of the HAAF framework was done in an environment in a real-life authentication situation. The simulation process was carried out in the following steps:

Step 1: Dataset Preparation

We used some datasets that are available to the public like FVC2004 which is for fingerprints and CASIA-Iris.

Step 2: Baseline System Implementation

Three authentication systems were implemented: traditional password-based authentication, Multi-Factor Authentication (password + OTP), and the proposed HAAF framework.

Step 3: Password Processing

User passwords were validated for complexity, transformed using the Braille encoding mechanism, and hashed using PBKDF2 or Argon2 for secure storage.

Step 4: Biometric Processing

Biometric inputs were pre-processed to remove noise and converted into stable cryptographic keys using fuzzy extractors.

Step 5: Adaptive Cryptography Simulation

A machine learning-based risk model used features such as login frequency, device ID, IP address, and failed login attempts to assess risk levels, dynamically increasing hash iterations and triggering additional authentication layers when necessary.

Step 6: Blockchain Layer Simulation

A simulated blockchain environment was used to store authentication logs and verify access through smart contract logic.

Step 7: Attack Simulation

The systems were tested against brute-force, dictionary, and replay attacks to evaluate their security and resilience.

Step 8: Performance Measurement

The following metrics were recorded:

- Execution Time (ms)
- FAR (False Acceptance Rate)
- FRR (False Rejection Rate)
- Throughput (requests/sec)

Step 9: Comparative Analysis

Results from all three systems were compared and visualized using graphs to evaluate improvements in security, accuracy, and efficiency.

M. EXPERIMENTAL SETUP

The evaluation of HAAF is conducted in a simulated environment designed to replicate real-world authentication scenarios.

Hardware Configuration: Multi-core processor with GPU acceleration for testing password cracking resistance.

Software Tools: Python-based cryptographic libraries, machine learning frameworks, and blockchain simulation tools.

Datasets: Fingerprint dataset (FVC2004), Iris dataset (CASIA-Iris)

Hashing Algorithms Tested: PBKDF2, bcrypt, and Argon2

Baseline Systems:

- Traditional password-based authentication
- Standard multi-factor authentication (Password + OTP)

N. EXECUTION TIME ANALYSIS

Execution time really matters in authentication systems. It affects how users feel when they try to get

in. The HAAF framework adds some steps. These include processing and adaptive cryptography. They make it take a bit longer to compute than traditional systems do. Execution time is really important here. The HAAF framework does make it a bit slower.

Figure 3 shows how long it takes for password-based systems, standard MFA and the proposed HAAF framework to do their job.

Although HAAF takes a bit longer to execute than authentication methods the extra time is worth it because it offers much better security, reliability and accuracy. The framework uses advanced security features like adaptive hashing, anomaly detection, biometric verification and blockchain validation which require more computing power. With the extra time it takes HAAF still works well in real-time authentication environments. The enhanced protection, against access, phishing attacks, credential theft and identity spoofing outweighs the minor delay introduced during the HAAF authentication process.

TABLE 1: EXECUTION TIME COMPARISON

System Type	Avg. Execution Time (ms)
Password Only	50 ms
Password + OTP (MFA)	120 ms
Proposed HAAF	180 ms

Figure 4 shows the False Acceptance Rate comparison. The proposed HAAF framework greatly reduces FAR. This means fewer unauthorized people can get in. It does this by combining authentication with a special kind of key generation.

Figure 5 shows that HAAF also keeps a False Rejection Rate. This means HAAF does not stop users from getting in very often.

Authentication Accuracy

Authentication accuracy is evaluated using FAR, FRR, and EER metrics.

The results show that HAAF makes a difference in reducing false acceptance and false rejection rates. This is because HAAF uses verification and fuzzy extractors together.

The analysis of how things the system can handle shows that HAAF handles a little fewer request every second compared to other systems.

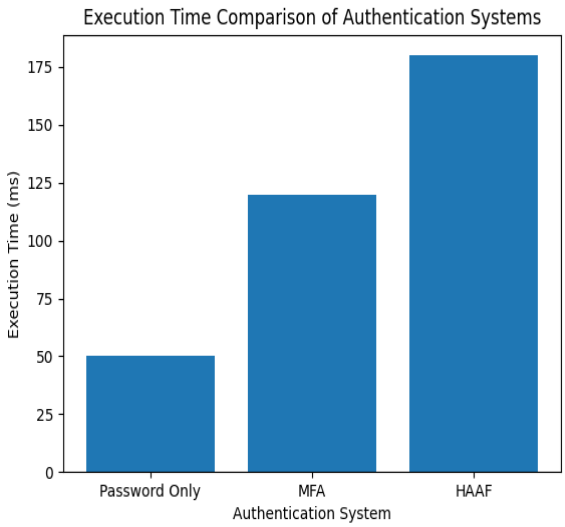

Fig 3: Execution Time Analysis

TABLE2: FAR COMPARISON (SECURITY ACCURACY)

System	FAR (%)
Password Only	5.2
MFA	2.1
HAAF	0.8

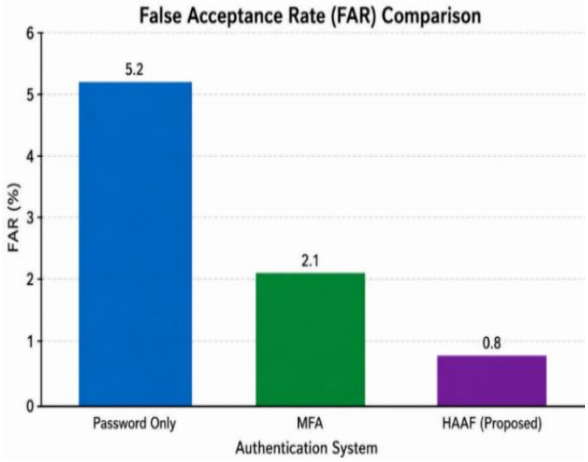

Fig 4: Far Comparison (Security Accuracy)

TABLE 3: FRR COMPARISON

System	FRR (%)
Password Only	3.8
MFA	2.5
HAAF	1.2

Security Strength Analysis

The security strength of HAAF is evaluated based on resistance to various attack types. The results show

that HAAF provides good protection against all major attack vectors because it has a lot of layers

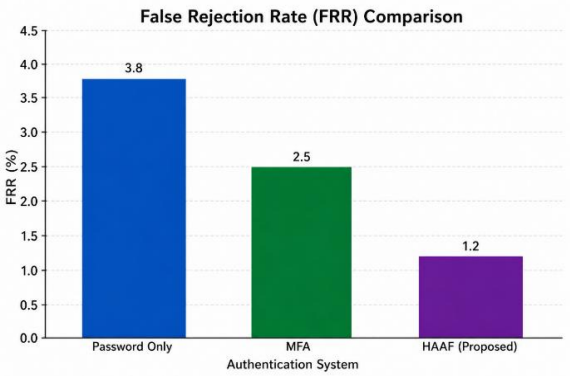

Fig 5: False Rejection Rate

TABLE 4: ACCURACY COMPARISON

System Type	FAR (%)	FRR (%)	EER (%)
Password Only	5.2	3.8	4.5
MFA (Password + OTP)	2.1	2.5	2.3
Proposed HAAF	0.8	1.2	1.0

TABLE 5: THROUGHPUT VS USERS

Users	Password	HAAF
100	500	420
500	450	390
1000	400	350

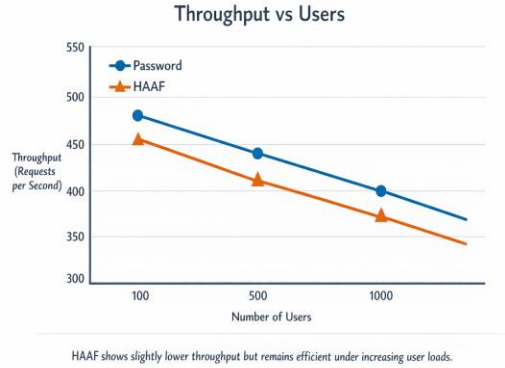

Fig 6: Throughput versus number of users

TABLE 6: ATTACK RESISTANCE COMPARISON

Attack Type	Password Only	MFA	HAAF
Brute Force	Low	Medium	High
Dictionary Attack	Low	Medium	High
Phishing	Low	Medium	High
Replay Attack	Medium	Medium	High
Biometric Spoofing	Not Applicable	Medium	High

Throughput and Scalability

The system is tested to see how well it works when more people use it at the time. This is done by increasing the number of users who are using the system at once.

The HAAF system is a little slower because it has steps to go through but it still works really well for big systems. The HAAF is good, for large-scale systems because it can handle a lot of work.

Adaptive Cryptography Performance

The machine learning based adaptive module changes how strong the encryption is when it finds something that might be a threat. The machine learning based adaptive module is always looking for threats. It changes the encryption strength to keep up with the machine learning based adaptive modules findings.

TABLE 7: THROUGHPUT ANALYSIS

Number of Users	Requests/sec (Password)	Requests/sec (HAAF)
100	500	420
500	450	390
1000	400	350

TABLE 8: ADAPTIVE RESPONSE

Threat Level	Hash Iterations	Authentication Mode
Low	10,000	Password + Biometric
Medium	50,000	MFA Required
High	100,000	Multi-layer + Blockchain

This ability to adapt means that security is made stronger when there are risks but it does not make things more complicated when everything is working normally. The security is strengthened in high-risk scenarios.

TABLE 9: OVERALL PERFORMANCE COMPARISON

Feature	Traditional	MFA	HAAF
Security Level	Low	Medium	Very High
Adaptability	No	Limited	Yes
Biometric Integration	No	Partial	Full
Blockchain Support	No	No	Yes
Privacy Protection	Low	Medium	High

Comparative Analysis with Existing Systems

The comparison clearly shows that HAAF does better than systems and MFA systems in every important way. HAAF is really good at what it does. It is better, than traditional systems and MFA systems when you look at the important things that matter.

Discussion of Results

The performance evaluation shows that our HAAF framework does a job of balancing security and efficiency. It does add some computing work because of its layered design. The benefits in terms of better authentication accuracy and protection against attacks make up for the extra time it takes. The use of authentication really helps to lower the number of false acceptances. Fuzzy extractors also help keep user data private. The Hybrid Adaptive Authentication Framework is more secure and accurate. It can handle a lot of work at the time, which makes it more adaptable for security requirements in the present day.

V. DISCUSSION

The Hybrid Adaptive Authentication Framework (HAAF) represents an advancement in authentication security by integrating multiple security mechanisms into a unified and flexible framework. Experimental results demonstrate that HAAF enhances security, improves authentication accuracy, and provides greater resistance against evolving cyber threats.

The use of fuzzy extractors improves authentication reliability by generating stable cryptographic keys from biometric data, reducing false acceptance and rejection rates. Machine learning enables adaptive security by monitoring user behaviour and dynamically adjusting authentication requirements when suspicious activities are detected. In addition, blockchain technology provides decentralized and tamper-resistant access control, ensuring data integrity and eliminating single points of failure.

Despite these advantages, the framework introduces higher computational overhead and increased system complexity. Authentication latency, dependence on biometric data quality, and the resource requirements of machine learning and blockchain components present implementation challenges. However, optimization techniques and advancements in lightweight blockchain and machine learning models can help overcome these limitations. Overall, HAAF provides a secure, adaptive, and privacy-preserving authentication solution that effectively addresses the limitations of conventional authentication systems and offers a promising approach for protecting digital identities in modern computing environments.

VI. CONCLUSION

The increasing sophistication of cyber threats has exposed the limitations of traditional password-based authentication systems, which are vulnerable to attacks such as phishing, brute-force, and credential stuffing. These challenges highlight the need for more secure and adaptive authentication mechanisms.

To address these issues, this study proposes a Hybrid Adaptive Authentication Framework (HAAF) that integrates Braille-based password transformation, biometric authentication, fuzzy extractor-based cryptographic key generation, machine learning-driven adaptive security, and blockchain-enabled access control. By combining multiple layers of security, the framework provides enhanced protection, improved accuracy, and greater resilience against evolving cyber threats.

The proposed HAAF represents a promising approach for developing secure, scalable, and privacy-preserving authentication systems suitable for modern digital environments.

REFERNCES

[1] A. S. J. L. S. S. K. Xinzhang Chen, "BeyondLife: An Open-Source Digital Will Solution for Posthumous Data Management," IEEE Access, vol. 13, pp. 99391-99414, 2025.

[2] H. K. e. al., "Secure Face De-Identification with Format-Preserving Encryption," IEEE Access, 2025.
[3] V. K. e. al., "Timestamp Based OTP and RSA Key Exchange for IoT Security," Journal of Cyber Security and Mobility, vol. 12, no. 14, 2023.
[4] S. N. K. Sasikumar, "Adaptive Cryptography Using Machine Learning," IEEE Open Journa, 2025.
[5] S. P. e. al., "Robust and Reusable Fuzzy Extractor for Authentication," IEEE Access, 2026.
[6] P. M. D. Palma, "Privacy-Preserving Retina Authentication," IEEE Access, 2024.
[7] B. R. e. al., "IDChat: Multi-Biometric Digital Identity System," IEEE Access, 2026.
[8] S. S. D. Kim, "Optimization of PBKDF2-HMAC-SHA2 Password Cracking on GPUs," IEEE Access, 2024.
[9] M. V. V. Dineshbabu, "SecureFLACF Blockchain Security Framework," IEEE Access, 2025.
[10] H. T. e. al., "Braille Transformation for Secure Password Hashing," IEEE Access, 2024.
[11] A. Saran, "Time-Memory Trade-Offs in Password Hashing," Frontiers in Computer Science, 2024.
[12] I. T. e. al., "Bloom Filter Approach for Password Cracking Efficiency," EURASIP Journal on Information Securit, 2024.
[13] M. A. e. al., "Fuzzy-Extractor-Based Hardware Authentication," Applied Sciences, 2024.
[14] A. I. e. al., "Secure Biometric Access Using Fuzzy Logic," IEEE Transactions on Reliability, 2021.
[15] N. S. J. Gowthami, "Fuzzy Extractor Based Authentication for Wearable Devices," Conference Publication, 2018.
[16] M. Y. e. al., "Lightweight Biometric Authentication for IoT Systems," IEEE Open Journal, 2024.
[17] A. A. e. al., "Quantum Secure Biometric Authentication Scheme," Soft Computing, 2026.
[18] S. P. S. P. A. K. J. M. Uludag, "Biometric Cryptosystems: Issues and Challenges," Proceedings of the IEEE, vol. 92, no. 6, pp. 948-960, 2004.
[19] M. W. Ari Juels, "A Fuzzy Commitment Scheme," ACM CCS, pp. 28-36, 1999.
[20] J. J. B. J. Paul Kocher, "Differential Power Analysis," CRYPTO, vol. 1666, pp. 388-397, 1999.