International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 18, Number 1 (2025), pp. 1 - 9
© International Research Publication House
http://www.irphouse.com

Enhancing Biometric Relay Attack Mitigation Using Cryptography and Blockchain

Prof. Megha M Veerkar
Dept. of ECE
Atria Institute of Technology
Bangalore, India
megha.mv@atria.edu.in

Husna Firdos
Dept of ECE
Atria Institute of Technology
Bangalore, India
husna.engg1104@gmail.com

Mayuri S Nayak
Dept of ECE
Atria Institute of Technology
Bangalore,India
mayurinayak16@gmail.com

Harmain Fathima Khan
Dept of ECE
Atria Institute of Technology
Bangalore, India
khanharmain646@gmail.com

Meghana A.P
Dept of ECE
Bangalore, India
meghanaap3225@gmail.com
Atria Institute of Technology

Abstract

Even though biometric authentication has grown to become a significant portion of secure access control systems, it still has narrow use cases because of possible replay attacks. By fusing cutting-edge blockchain technology with cryptography, the current work offers a novel approach to enhancing biometric authentication systems. The authentication process stays "dynamic" and the possibility of spoofing the biometric authentication system is nearly eliminated when the cryptographic variable keys are connected to the "live" biometric. With blockchain technology, blockchain storage becomes integrated and impenetrable, and access will become real-time. Removing centralized systems border tampering and unauthorized access risks, and allows instant access. The system's objective is to offer biometric authentication systems that are reliable, scalable, and privacy-preserving.

Keywords: Biometric authentication, replay attack mitigation, cryptographic key binding, blockchain security, decentralized identity management, privacy-preserving authentication.

I. Introduction

The physical and virtual borders of identity are now more pervious in the digitally transforming times. The need for reliable and user-friendly authentication methods has never been higher due to the growth of online services, financial systems, and online-connected devices. Using distinctive human characteristics like fingerprints, facial features, or iris scans, biometric authentication has emerged as a key component of contemporary identity authentication. Unlike traditional credentials like passwords or tokens, biometrics have built-in resistance to theft and forgetfulness, making them easy and reliable methods of gaining access to important systems.

But as adoption rises, so does the attack surface. Despite their ease of use, biometric systems still give rise to privacy and security issues. Unlike passwords, the use of biometric identifiers cannot be stopped or changed. Replay attacks, template theft and database attacks expose users to the inopportune risks of identity loss and impersonation. This issue is made worse by centralized storage designs, which introduce single points of failure and unsustainable trust dependencies into distributed and large-scale ecosystems. [7] [8] [9]. The new category of solutions, which includes both technological complexity and decentralization of the architecture, is required for the integrity and privacy of the biometric data, which is intimately linked to the individual's identity.

Blockchain and cryptography are solutions to these weaknesses. Immutability, distributed audit trail, and consensus-based trusted of blockchain reduces single points of failure, and two of eight cryptographic assurances over data integrity, freshness, and non-repudiation are assured by zero-knowledge proofs, key-binding, and digital signatures, respectively [1][2][3]. Some design strategies have been blown up by earlier research. With the help of template splitting and distributed management via BDAS, fragmentation and permissioned blockchains remove single points of failure [9]. Biometric feature extraction and matcher modules were decentralized using a weighted PBFT consensus to boost resilience against direct attacks [7]. Utilizing zero-knowledge proofs and Monero's privacy features, privacy-sensitive authentication systems have been implemented in healthcare settings to provide a privacy-compliant solution that uses the right organizational and technological safeguards to protect personal data [8].

In the area of face recognition, biometric identity management on smart contracts has demonstrated efficacy with low error rates [5]. In order to create biometric-bound private keys using a cryptographic approach, it has been suggested to combine facial features with a hardware security primitive that uses the distinct, inherent physical variations of a device to create a unique and unclonable digital key [6]. Blockchain/Interplanetary File System-based multimodal biometric fuzzy vaults have demonstrated high accuracy and resilience against collusion and brute-force attacks [4]. Automated traffic classifiers and the blockchain+ cryptographic algorithm are effective in preventing key invalidation attacks in the Internet of Things environment [3]. At the edge network scale, blockchain-based authentication protocols offer continuous, lightweight authentication that has been shown to be secure in replay and impersonation [2].

This is also the direction of current trends. Sarier [10] presented a workable biometric-based identity management system for smart industrial settings that provides non-transferability through a newly computed disguised biometric attribute produced by a fuzzy extractor for each authentication. It will consist of off-chain storage and blockchain accumulators to satisfy the data protection, scalability and auditing requirements, respectively, to show that privacy-preserving biometric-based identity can be achieved without exposing the raw biometric data. The latter highlights technique emphasizes the greater promise of biometric liveness with cryptographic freshness, decentralized verification, and augmentation of digital identity.

These advances will not withstand, the majority of the systems still aim at protecting templates, distributed management, or generation of fixed key, none of which take into account the cryptographic binding of live biometric input to short-lives authentication or leveraging blockchain for immutable and decentralized verification. This vulnerability makes replay and spoofing attacks not to be properly dealt with.

To overcome these limitations, the present studies focuses on the following **objectives**:

1. **To design a cryptographic mechanism that dynamically binds authentication keys to live biometric inputs, ensuring freshness and preventing replay-based spoofing.** This aims at real-time biometric collection and cryptographic nonce or timestamp fusion to dynamically generate session keys. Every authentication attempt generates a distinct, verifiable key that is not reusable and replay able, thereby ensuring liveliness and session freshness while authenticating an individual.
2. **To integrate blockchain technology for decentralized storage and verification, providing immutability, transparency, and distributed trust without exposing raw biometric data.** This uses the blockchain decentralized ledger for storage of hashed biometrics and verification proofs and not the sensitive biometrics. This will combine cryptographic techniques for biometric data with a privacy- preserving decentralized blockchain to eliminate centralized biometric privacy- exposed insider threats and points of failure.

The goal is to develop a strong, scalable, and privacy-preserving authentication system that ties live biometric data with a temporary cryptographic key and locks verification within a blockchain record. By combining dynamic biometric cryptography with decentralized systems, the framework aims to eliminate the ongoing security disparity between the convenience offered by biometrics and the assurance provided by cryptography, setting a new benchmark for seamless and secure user authentication.

II. MATERIALS AND METHOD

A. MATERIALS

The proposed biometric-based authentication framework was developed using Python 3.13 in the Spyder IDE (Anaconda environment). The primary Python libraries utilized in the implementation include:

- Cryptographic Hash Library (SHA-256)
- System Software – for secure random number (nonce) generation.
- Time for timestamp generation and session monitoring.

The system was implemented on a Windows 11 (64-bit) operating system running an Intel Core i5 processor and an 8 GB RAM. Because the mechanism of security was the subject of this research, the simulated input of the user was represented as synthetic biometric data instead of actual biometric sensors. Individual simulated input string (for example, UserFingerprintScan123) represents biometric features extractable from actual biometric modality like fingerprints or facial scans.

B. METHOD

The suggested algorithm combines biometric feature hashing and session key generation with blockchain-based replay protection in order to provide secure and tamper-proof authentication.
The process is divided into two main phases: Session Key Generation and Blockchain-Based Session Validation.

1. SESSION KEY GENERATION

In this phase, a unique cryptographic session key is generated for each user authentication attempt. The steps involved are:

- **Step 1:** Biometric Feature Extraction. The biometric input or biometric building block is converted into a fixed-length 256-bit hash using the SHA-256 algorithm:

  $F=H(B)$ ------------------ (1)

  where F represents the extracted biometric feature.
- **Step 2:** Nonce Generation. A random 16-byte nonce NNN is generated using the os.urandom () function:

  N=os.urandom(16).hex() ----- (2)

This random nonce ensures that every authentication instance is unique and resistant to replay attacks.

- **Step 3:** Session Key Derivation. The session key is obtained by concatenating the biometric feature and nonce, followed by SHA-256 hashing as follows**:**

  $S=H(F \mid\mid N)$ -------------- (3)

where || denotes concatenation. The resulting session key is unique for each session, even for the same biometric input.

2. BLOCKCHAIN-BASED SESSION VALIDATION

To ensure immutability and detect replay attempts, the session key is validated and recorded within a private blockchain.

- **Step 1:** Session Key Hashing before recording, the session key is hashed again to produce a session hash H_s:

  $H_s=H(S)$ ------------------ (4)
- **Step 2:** Block Formation each new authentication attempt creates a block containing the session hash, timestamp T, block index i, and hash of the previous block P:

  $B_i=H(i \mid\mid H_s \mid\mid T \mid\mid P)$ ----- (5)

This block structure guarantees the integrity and chronological order of the authentication events.

- **Step 3:** Replay Detection the blockchain verifies whether H_s already exists in previous blocks:

  If $H_s \in \text{Chain} \Rightarrow$ Replay Attack Detected -- (6)

Otherwise, a new block is appended, marking a valid authentication session.

- **Step 4:** Integrity Verification during each session, block hashes are recomputed and compared with the stored values to confirm data integrity and prevent tampering.

C. EXAMPLE IMPLEMENTATION

A sample execution using the simulated biometric input *"UserFingerprintScan123"* yielded the results shown in Table 1:

Parameter	**Example Output**
Biometric Feature (F)	9356eaa296fea01087d6486783d34c3059289c6b797a5ec80fef7596c24c176e
Nonce (N)	abc6893a3b9f2cb9095c783c81501c62
Session Key (S)	8451f3728f2036e8c9c549fe4ad6a780be7e87398b6b27d5884a8902ac697d36
Session Hash (H_s)	0b7f6e07ae94545e5072ff46bc2bb1bd0d42e644583f2cdb5cee6ab37475fa4c

Table 1

A new block was generated with the following hash:

$B_1=H(1 \,||\, H_s \,||\, 1700000000 \,||\, 0)$=e8b93f907b43000880793e569cc6fd8
68716a958da4ce450576fe4210aa47ef ---------------------------- (7)

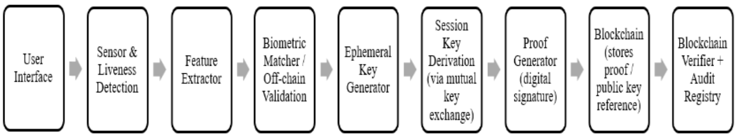
The subsequent reuse of the same session key triggered a “Replay Detected” message, validating the proposed security mechanism.

D. SUMMARY OF THE WORKFLOW

1. Capture biometric data (simulated input)
2. Extract biometric features via SHA-256 hashing
3. Generate random nonce for each session
4. Compute session key and session hash
5. Record session hash in blockchain
6. Verify authenticity and detect replay attempts

III. Block diagram

In order to achieve the two key research objectives, the suggested framework (as represented in the block diagram) combines both biometric cryptography and blockchain verification. It starts at the user interface where live biometric data are collected and verified in terms of liveness to stop spoofing. Ephemeral key generator processes extract features and generate a unique session key based on the live biometric input, making it fresh and resistant to a replay attacks. An off-chain matcher checks this key and the extracted features, and a proof generator generates cryptographic, a hash or a zero-knowledge proof without exposing raw biometric data. Authenticated evidence is then stored within the blockchain and offers immutable, decentralized validation and auditability. The verifier of blockchain verifies every transaction by consensus and the audit registry keeps transparent and immutable logs of transactions to provide long-term trust and compliance


User Interface
Sensor & Liveness Detection
Feature Extractor
Biometric Matcher / Off-chain Validation
Ephemeral Key Generator
Session Key Derivation (via mutual key exchange)
Proof Generator (digital signature)
Blockchain (stores proof / public key reference)
Blockchain Verifier + Audit Registry

.

Figure 1

IV. Methodology

The suggested methodology guarantees a secure and uncompromised biometric authentication process by combining two important security mechanisms: session key generation and binding and blockchain verification. In order to guarantee key reuse or replay, the former uses the creation of a time-sensitive, distinct session key that is cryptographically fixed to the user's real-time biometrics. The second plan uses blockchain technology to track and authenticate each authentication request in a decentralized manner. Only when the session key is confirmed to be unique is a new block added to the block chain; if a duplicate key is found, it signals a relay attack, and that delivery is simply rejected.

Together, the two elements provide the advantages of two-layered security, ensuring both the unchangeable ability of transaction verification and the temporal freshness of biometric data.

A cryptographic connection between biometric inputs and the authentication session is established by the session key protocol generation. In order to provide a temporary key that is only valid once, each session would require real-time biometric input and an exclusive timestamp.

A. SESSION KEY GENERATION AND BINDING

1) Biometric Feature Extraction

A secure sensor receives a biometric input (for example, a fingerprint, a face) from the user. A fuzzy extractor converts biometric information to a reproducible representation while remove noise and interscan variability. This ensure that the same user generates a similar yet safe pattern every time without the storage of the raw biometric template.

2) Session Key Generation

one-way hash function is used to derive a session key by combining the biometric features with a timestamp. This will ensure that although the same biometric data are reused, each session key unique due to the varying timestamp.

3) Key Binding

Next, the binding are cryptographically bound to the session key and digital signature with the device secret key is performed. The transaction containing the signed session key is coded in a transaction that is forwarded to the blockchain verifier. This binding guarantee authenticity by conforming that the session key originates from a legitimate biometric device.

4) Ephemeral Key Property

The generated session key is temporary, that is, it has a short duration, or dies after use or time elapse. Thus, if an attacker steals the key or the encrypted packet, it becomes unusable in any subsequent session.

B. BLOCKCHAIN VERIFICATION AND RELAY ATTACK MITIGATION

The second defense mechanism is the blockchain verification method. This ensures that all authentication requests are authenticated, logged and verified in a decentralized fashion without the need of centralized trust.

1) Transaction Creation

The device sends a transaction which carries the hash of the session key, device identifier, time and evidence of biometric binding. This is then transmitted to each node of the blockchain.

2) Uniqueness Verification

Each blockchain node verifies the existence of the received session key (or the hash of the session key) in the ledger.

- If the key is new, the transaction is considered valid and a new block is generated.
- When the key is repeated, it indicates a relay/replay attack. The transaction is declined, and the occurrences are registered in the audit and revocation registry.

3) Consensus and Block Addition

After verification, the nodes agree and append the transaction to the blockchain as a new block. Owing to blockchain immutability, no block can ever be altered or overwritten, ensuring that authentication logs will have integrity even in the long-run.

4) Audit and Revocation Registry:

Failed and duplicated attempts are recorded in an off-chain audit registry so that the administrator can trace anomalies and revoke compromised devices when necessary.

5) Security Outcome:

The immutability of blockchain and uniqueness of session keys make the system such that each authentication is irreversible and verifiable and resistant to interception. The attacks that fail to work due to relaying is that any replayed or delayed version of the session key is instantly detected as a duplicate version and rejected by the blockchain validator.

This two-layered strategy efficient to make biometric authentication systems more hardened. They combine and provide a safe, open, decentralized system that can identify and avert relay attacks in real-time without violating user privacy by not placing the raw biometric information on-chain

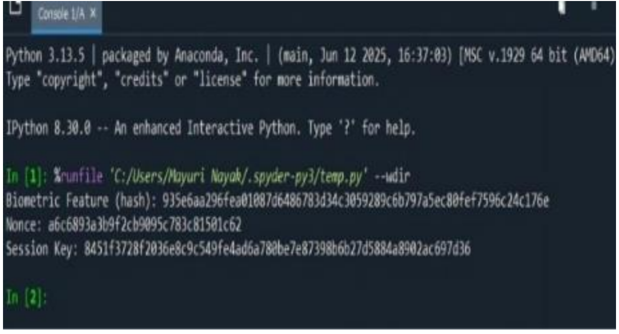
V. Result and discussion

The model employing biometric session key generation and blockchain integration was implemented in Python language. The experiments were conducted to test the ability of the system to assure the enforcement of secure session formation and replay assaults by means of decentralized verification.

A. SESSION KEY GENERATION ANALYSIS

The system has a two-step hashing scheme in which the biometric data is subjected to the first step processing by the SHA-256 algorithm in order to extract distinct biometric features. Each time an authentication attempt is made a 16-byte cryptographically secure random nonce is made to guarantee that every attempt is unique. The result is then the generation of the session key, which is obtained by concatenating the nonce and the hash of the biometric feature, and then another round of SHA-256.

An example output of the implemented module is shown below in figure 2:



```
Python 3.13.5 | packaged by Anaconda, Inc. | (main, Jun 12 2025, 16:37:03) [MSC v.1929 64 bit (AMD64)
Type "copyright", "credits" or "license" for more information.

IPython 8.30.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: %runfile 'C:/Users/Mayuri Nayak/.spyder-py3/temp.py' --wdir
Biometric Feature (hash): 935e6aa296fea01087d6486783d34c3059289c6b797a5ec80fef7596c24c176e
Nonce: a6c6893a3b9f2cb9095c783c81501c62
Session Key: 8451f3728f2036e8c9c549fe4ad6a780be7e87398b6b27d5884a8902ac697d36

In [2]:
```

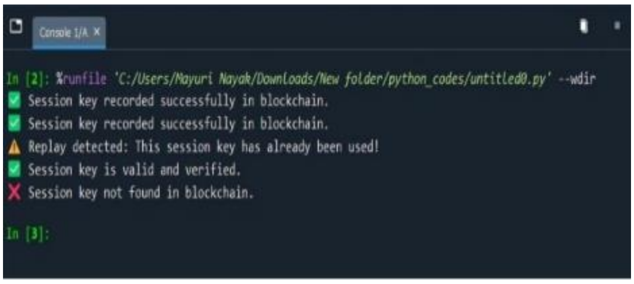
Figure 2

The findings confirm that even when the same biometric input is reused, a dynamically generated nonce ensures that each instance will have a different session key. This helps to deter key replication and augment session-based confidentiality.

B. BLOCKCHAIN-BASED AUTHENTICATION AND VALIDATION

Every session is recorded on the blockchain as a new block containing the session key hash, timestamp, and the hash of the preceding block. The genesis block is set on system initiation and appendage of each subsequent block is done in turn with successful session validation.

The blockchain was tested against repeated and new session key inputs. The following output was observed in figure 3:



```
In [2]: %runfile 'C:/Users/Mayuri Nayak/Downloads/New folder/python_codes/untitled0.py' --wdir
✅ Session key recorded successfully in blockchain.
✅ Session key recorded successfully in blockchain.
⚠ Replay detected: This session key has already been used!
✅ Session key is valid and verified.
❌ Session key not found in blockchain.

In [3]:
```

Figure 3

The system successfully detected and blocked replay attempts, thereby confirming the robustness of the blockchain verification mechanism. This decentralized structure eliminates the dependency on a single authentication authority, making the system resilient against tampering and unauthorized data modification.

C. SECURITY AND PERFORMANCE DISCUSSION

Bio-data and blockchain can be joined, which offers two-level security.r The biometric feature extraction provides user-specific identity verification and blockchain immutability assures that the key features of the recorded sessions cannot be modified and used again. SHA-256 hash algorithm provides a one-way mapping that is computationally hard, and this makes it impossible to reverse engineer session keys.

Experimental evaluation indicates that:

- The nonce-based entropy creates a unique session key each time there is an authentication request.
- Blockchain verification is a valid method of replay attacks.
- The computational overhead is also low as both the computation of SHA-256 and the generation of the nonce are lightweight.

This hybrid approach provides superior integrity, transparency, and security of user authentication systems over traditional centralized password-based methods.

VI. Conclusion

This system combines biometric authentication with blockchain technology for even greater security while using biometric data for session key generation and authentication. SHA-256 hashing with nonce-based session key generation guarantees that session keys will be unique and prevents replay duplication. Authentication sessions that take place in real-time are logged on the blockchain ledger, and the system can conduct real-time replay-attack forgery prevention as well. This approach works for the secure verification of identity in a decentralized, tamper-proof, and computationally efficient manner. Future work could address efficient consensus solutions designed for widespread IoT integration and multi-user scalability. In comparison to each other, the session key-based authentication is an assurance of freshness and dynamic identity binding, though it depends on the secure key management and can be threatened using the same method should the verification database be hacked. The authentication based on blockchain, however, is immutable, decentralized, and transparent yet cannot be adaptable in real-time without a secure source of input. The integration of session key generation with blockchain technology forms a hybrid model that delivers superior security; the session key provides freshness and user-specific assurance, while the blockchain ensures tamper-proof and irreversible verification.

VII. **Reference**

[1] W. Zhou, D. Lyu, and X. Li, “Blockchain security based on cryptography: A review,” arXiv preprint arXiv:2508.01280, 2025.

[2] A. Iftikhar, K. N. Qureshi, F. B. Hussain, M. Shiraz, and M. Sookhak, “A Blockchain-based Secure Authentication Technique for Edge-based Smart City Networks,” Journal of Network and Computer Applications, vol. 240, pp. 104–121, 2025.

[3] S. H. Gopalan, A. Manikandan, N. P. Dharani, and G. Sujatha, “Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks,” International Journal of Networked and Distributed Computing, vol. 12, no. 1, pp. 45–58, 2024.

[4] S. Sharma, A. Saini, and S. Chaudhury, “Multimodal Biometric User Authentication Using Improved Decentralized Fuzzy Vault Based on Blockchain,” Journal of Information Security and Applications, vol. 78, pp. 103–118, 2024.

[5] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, “Blockchain-based Biometric Identity Management,” Cluster Computing, vol. 26, pp. 1763–1778, 2023.

[6] Y. Wang, B. Li, Y. Zhang, J. Wu, G. Liu, Y. Li, and Z. Mao, “A Novel Blockchain Private Key Generation Mechanism Using Facial Biometrics and Physically Unclonable Functions,” Journal of Information Security and Applications, vol. 73, pp. 102–115, 2023.

[7] M. Žiška, “Biometric System Security Using Blockchain Technology,” Bachelor’s Thesis, Brno University of Technology, Faculty of Information Technology, 2022.

[8] N. D. Sarier, “Privacy Preserving Biometric Authentication on the Blockchain for Smart Healthcare,” Pervasive and Mobile Computing, vol. 84, 2022.

[9] Y. K. Lee and J. Jeong, “Securing Biometric Authentication System Using Blockchain,” ICT Express, vol. 7, no. 4, pp. 431–435, 2021.

[10] N. D. Sarier, “Efficient biometric-based identity management on the Blockchain for smart industrial applications,” Pervasive and Mobile Computing, vol.79,pp.101491,202