I.J. Wireless and Microwave Technologies, **2026, 3, 142-159**
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.03.10

Enhancing Cloud Storage Security Using Multi-User Biometric Encryption with Threshold Access Control

Sahil Rampal
School of Computer Application, Lovely Professional University, Phagwara-144411, Punjab, India.
E-mail: sahil.rampal@gmail.com
ORCID iD: 0000-0001-5786-9039

Manmohan Sharma
School of Computer Application, Lovely Professional University, Phagwara-144411, Punjab, India.
E-mail : manmohan.sharma71@gmail.com
ORCID iD: 0000-0001-9445-5898

Parul Khurana
Department of Computer Science & Applications, Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, Uttar Pradesh – 201310, India.
E-mail : parul11183@gmail.com, parul.khurana@sharda.ac.in
ORCID iD: 0000-0002-3232-6983

Mukesh Kumar*
[1]Advanced Centre of Research & Innovation (ACRI), School of Advance Computing, CGC University Mohali-140307, Punjab, India.
[2]Faculty of Law, Sohar University, Solar, Sultanate of Oman.
E-mail: mukesh.kumarphd2014@gmail.com,
ORCID iD: 0000-0001-8797-9810
***Corresponding Author**

Received: 09 April 2025; Revised: 25 March 2026; Accepted: 09 May 2026; Published: 08 June, 2026

Abstract: Cloud computing has become an essential platform for business data storage and application management due to its scalability, accessibility, and cost-effectiveness. However, ensuring the security and privacy of sensitive cloud data remains a major challenge because cloud users do not have direct control over their stored information. Traditional single-biometric encryption approaches often suffer from issues such as biometric variability, spoofing risks, and single-point failure. To address these limitations, this paper proposes a multi-user multi-modal biometric encryption framework integrated with threshold-based access control for securing business data stored in cloud environments. In the proposed approach, fingerprint and audio biometric modalities are pre-processed to extract privacy-preserving feature vectors, which are fused to generate individual user-keys using a Hash-Based Key Derivation Function (HKDF). Subsequently, a master encryption key is generated through Shamir's Secret Sharing and Lagrange interpolation mechanisms, where only a predefined threshold number of valid user-keys can reconstruct the master key for decryption. AES symmetric encryption is employed to secure the business data before cloud storage. Experimental evaluation was performed using the FVC2002 fingerprint dataset and Mozilla CV-Corpus audio dataset. The generated biometric master-key successfully passed Shannon Entropy, Chi-Square, Monte Carlo Pi, and decryption validation tests, demonstrating improved randomness, reliability, and resistance against unauthorized access. The proposed framework effectively eliminates single-point failure issues and enhances secure cloud data access through threshold-based biometric authentication.

Index Terms: Biometric Encryption, Cloud Security, Multi-Modality Solutions, Biometric Encryption, Cryptography, Biometric Decryption

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

1. Introduction

Although cloud computing platforms employ several advanced security mechanisms, concerns related to data confidentiality, insider threats, unauthorized access, and key management still remain significant challenges, particularly for sensitive business applications. Existing encryption-based solutions improve data protection; however, single-factor or single-biometric approaches may suffer from issues such as biometric variability, spoofing risks, and single-point failure. Therefore, there is a need for more robust multi-user and multi-modal security frameworks capable of enhancing secure access control and distributed trust in cloud environments. Recent reports from the Cloud Security Alliance (CSA) continue to identify data breaches, insider threats, and account hijacking as major security concerns in cloud environments. Furthermore, cloud user leverages the benefits of extending their hardware requirements without making provisioning plans to add up additional hardware to keep up the initiative. These benefits led to more successful business start-ups. However, as the utilization of cloud services continues to grow, so do the challenges associated with it. One of the most pressing issues is security. The increasing number of cyber-attacks targeting cloud infrastructures has raised serious concerns about the safety and integrity of data stored in the cloud. Every cloud service breach cost very high to the cloud provider and cloud users. All the currently available public, private, community or hybrid cloud systems do not have any strong form of security; as a result, cloud users are reluctant to store their confidential data on the cloud. The biggest challenge in cloud computing is data security from hackers and the malicious cloud service providers. Although many attempts are made to secure the cloud data, hackers are still able to breach the cloud security. Data encryption-based solutions implemented at cloud also failed to save the data while data in transit or when cloud service provider is malicious. Therefore, we purpose multi-key, multi-modality biometric encryption scheme to secure the data at local premises or offloading to the cloud.

Although several biometric encryption and cloud security approaches have been proposed in the literature, most existing methods rely on single-biometric modalities or single-user authentication frameworks. Such approaches are susceptible to biometric variability, spoofing attacks, and single-point failure due to centralized key dependency. Furthermore, limited attention has been given to integrating multi-user threshold-based cryptographic access control with privacy-preserving multimodal biometric fusion for secure cloud data storage. Therefore, there exists a need for a robust framework capable of combining distributed trust, multimodal biometric authentication, and threshold-based master-key generation to improve cloud data security and access reliability. The primary contribution of this work lies in combining multi-user multimodal biometric fusion with threshold-based cryptographic key reconstruction for secure cloud storage. Unlike existing single-biometric or single-user systems, the proposed framework distributes trust among multiple authorized users and enhances resistance against single-point failure, biometric compromise, and unauthorized cloud access.

In the proposed system, data is encrypted using a master encryption key obtained by integrating all the user-keys, which are formed by fusing the users' multiple biometric feature vectors generated from various modalities. The rest of the paper is organized as follows. Section 2 Literature Review Section 3 Proposed Methodology Section 4 Experiment and Results. Section 5 Conclusion and future Scope.

2. Literature Review

Cloud computing has emerged as a dominant paradigm for scalable storage, distributed processing, and on-demand service delivery. According to the National Institute of Standards and Technology (NIST), cloud computing enables ubiquitous and convenient access to shared configurable computing resources with minimal management overhead [1]. Despite its advantages, cloud computing environments continue to face significant security and privacy challenges, particularly related to data confidentiality, unauthorized access, insider threats, and distributed trust management [4], [8-12]. Recent studies have proposed several cryptographic and access-control-based mechanisms to enhance cloud security. Sinha et al. [2] introduced a functional-based stream cipher integrated with attribute-based access control and multiparty authorization to strengthen cloud data protection. Similarly, Garigipati et al. [3] proposed a poly-quantum integrity key generation framework for secure multi-user access control in cloud-based electronic health record systems. Although these approaches improve encryption and authorization mechanisms, they mainly depend on traditional key-management strategies and do not integrate biometric-based distributed trust models. Several blockchain-enabled and decentralized security frameworks have also been developed for secure cloud communication and storage. Murala and Thammireddy [5] proposed a multi-user integrity and multi-level attribute encryption framework for audio blockchain communication systems. Nalluri et al. [7] developed a blockchain-based multi-factor access control framework for preserving privacy in medical cloud storage systems. Likewise, Neela [20] presented a decentralized secure data outsourcing framework using hybrid encryption and blockchain smart contracts for cloud access control. While these approaches improve decentralization and transparency, they often introduce increased computational complexity and limited usability for practical multi-user biometric authentication systems.

Biometric authentication has gained considerable attention due to its capability to provide identity-based security and eliminate dependence on conventional passwords. Early studies by NIST [13] and Ross and Jain [14] demonstrated the effectiveness of biometric technologies for secure personal authentication and information fusion. Jagadiswary and

Saraswady [21] proposed a fused multimodal biometric authentication system to improve recognition accuracy compared with uni-biometric systems. Similarly, Hammad et al. [22] developed a convolution neural network-based multimodal biometric authentication system using ECG and fingerprint fusion. These multimodal approaches improve authentication reliability; however, most existing systems focus mainly on user authentication rather than cryptographic key generation and secure cloud storage protection. Recent advancements in biometric-cloud security integration have attempted to combine encryption with biometric authentication. Hammed et al. [6] proposed a decentralized cloud security framework utilizing biometric authentication and encryption mechanisms. Barman et al. [17] designed a secure crypto-biometric credential update protocol for multi-server environments. Ramya et al. [14] further explored multi-factor authentication with optimized encryption algorithms to enhance cloud security. Although these approaches improve authentication and encryption efficiency, they generally rely on single-user or centralized key structures, making them vulnerable to single-point failure and key compromise.

Hybrid cryptographic and multi-cloud data-sharing approaches have also been explored. Bharot et al. [16] introduced a hybrid cryptosystem for secure data sharing in multi-cloud environments, whereas Adeoye and Adams [18] proposed a hybrid post-quantum cryptographic and blockchain-based framework for scalable cloud security in IoT-enabled systems. Cai et al. [19] investigated authenticated encryption with keyword search for multi-user cloud scenarios. Despite these advancements, limited research has focused on integrating threshold-based cryptographic reconstruction with multimodal biometric fusion for distributed cloud access control. From the existing literature, it is evident that most prior studies either focus on cryptographic cloud security, blockchain-enabled access control, or biometric authentication independently. Limited attention has been given to combining multi-user multimodal biometric fusion with threshold-based master-key generation for secure cloud data protection. Furthermore, many existing approaches suffer from issues such as biometric variability, centralized trust dependency, lack of distributed access control, and vulnerability to single-point failure. Therefore, this study proposes a multi-user multi-modal biometric encryption framework integrated with threshold-based cryptographic reconstruction to enhance cloud data confidentiality, distributed trust, and secure access management.

Existing biometric encryption approaches have demonstrated effectiveness in authentication and access control; however, many studies rely on single-biometric modalities, making them vulnerable to spoofing attacks, biometric noise, and feature variability. Similarly, several threshold cryptographic systems focus primarily on secret sharing mechanisms without integrating privacy-preserving multimodal biometric fusion. Moreover, many existing cloud security solutions depend on centralized key management, increasing the risk of single-point failure and unauthorized access. These limitations indicate the need for a more robust framework that combines distributed trust, multimodal biometrics, and threshold-based cryptographic reconstruction for secure cloud data protection.

3. Proposed Methodology

In this competitive world, businesses require strict security practices to be followed for the data security. Businesses using cloud to store their data are heavily targeted by the hackers. Thus, there is a need to design a system where we can easily set the responsibility for the operation performed and to secure the data. Hence, we purpose multi-key multi-modality biometric encryption scheme, where selected biometric traits of multiple users are used to generate the master encryption key.

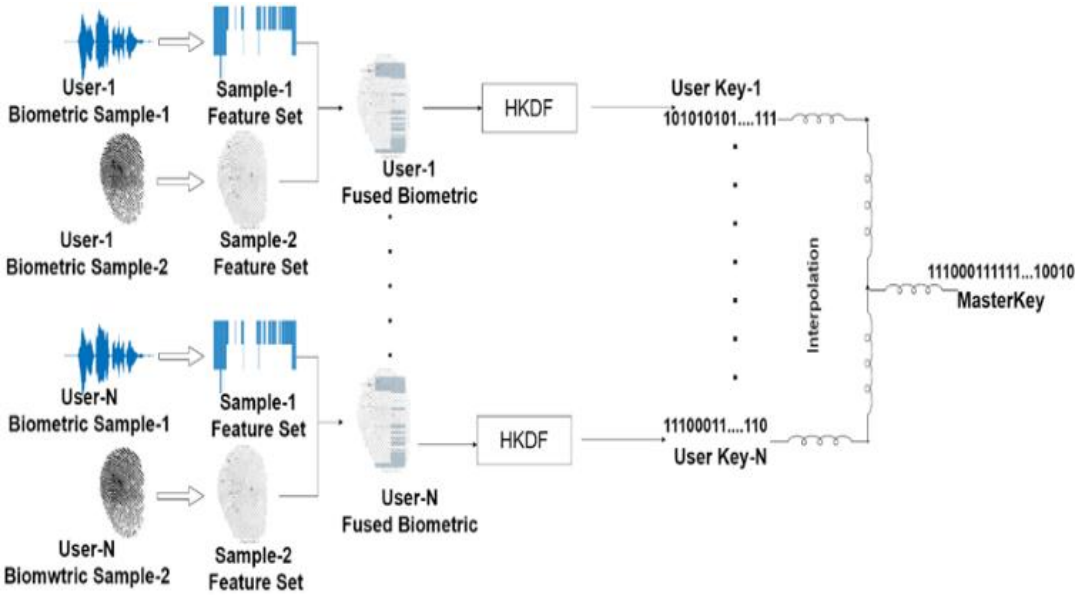


Fig. 1. Multi-Key multi-modalities key generation

Fig. 1., depicts the process to generate multi-key multi-modality biometric encryption key (Master-Key). firstly, biometric samples of various users (ensuring atleast one cancellable and at-least one fixed biometric) are acquired and supplied to the system for pre-processing, irreversible features templates are extracted from pre-processed biometric samples to preserve the user's privacy. user-keys are derived from the feature templates, those user-keys are interpolated to generate the master-key.

3.1. Multi-Key multi-modalities biometric key generation:

Multi-modalities biometric encryption keys (user-keys) are generated for data users, and user-keys are interpolated to generate the master key by Shamir's secret sharing approach by deciding the minimum number of keys (threshold) required to regenerate the master key. polynomial of degree $t-1$ where $f(x)= a^0+ a^1x + a^2x^2+ \dots + a_t{}^{-1}x^{t-1}$ is used to generate multi-modalities encryption key (master key), such that any sub group of threshold number of valid user-keys can be used to regenerate the master key.

- AcquireBiometricData(): For each individual data user: Acquire multiple biometric modalities such as fingerprint and audio (ensure that one of the biometric modalities is cancellable)
- PreprocessBiometricData(): For each acquired biometric modality: Preprocess the biometric data to prepare it for feature vector extraction for each data user:
- ExtractFeatureVectors(): Extract irreversible feature vectors from the pre-processed biometric modalities while preserving user privacy
- ApplyAudioSalting(): Apply audio salting by adding semi-random noise to the audio feature vector
- FuseFeatureVectors(): Fuse the feature vectors extracted from different biometric modalities for data user
- DeriveUserKey(): Derive a user-key from the fused biometric modalities of the data user using HKDF
- DeriveMasterKey(): Using Lagrange interpolation: Derive a master cryptographic key from all the user-keys (where n is the count of the data users and t is threshold), Record the polynomial coefficients.

Algorithm 1: Multi-User Multi-Modal Biometric Key Generation

1. Acquire fingerprint and audio biometric samples from all authorized users.
2. Preprocess biometric samples using normalization and noise reduction techniques.
3. Extract fingerprint minutiae and MFCC-based audio features.
4. Normalize extracted feature vectors.
5. Concatenate normalized feature vectors to generate fused biometric representation.
6. Apply HKDF-SHA256 to derive individual user-keys.
7. Generate threshold shares using Shamir Secret Sharing.
8. Construct the master-key through polynomial interpolation.
9. Encrypt cloud data using AES symmetric encryption.

3.1.1. Formal Feature Fusion Model

To generate a robust and privacy-preserving multimodal biometric representation, fingerprint and audio biometric features are extracted independently and later fused into a unified feature vector. Let the fingerprint feature vector extracted from minutiae points be represented as:

$$[F_\{fp\} = \{f_1, f_2, f_3, ..., f_m\}]$$

where (m) represents the total number of extracted fingerprint features. Similarly, the Mel-Frequency Cepstral Coefficient (MFCC)-based audio feature vector is represented as:

$$[F_\{au\} = \{a_1, a_2, a_3, ..., a_n\}]$$

where (n) denotes the total number of extracted audio features including MFCC, delta MFCC, and delta-delta MFCC components. To maintain consistency and reduce feature-scale variations, both biometric feature vectors are normalized using min-max normalization:

$$[F' = \frac\{F - F_\{min\}\}\{F_\{max\} - F_\{min\}\}]$$

where (F_{min}) and (F_{max}) represent the minimum and maximum values of the feature vector respectively. The normalized fingerprint and audio features are fused through feature-level concatenation to construct the multimodal biometric representation:

$$[F_\{fusion\} = [F'\{fp\} \,||\, F'\{au\}]]$$

where (||) denotes vector concatenation. The fused feature vector combines the discriminative characteristics of both modalities and improves robustness against spoofing, noisy inputs, and single-biometric failure. Multi-key multi-modalities biometric encryption can secure the data of businesses to be stored at cloud and fix the operation responsibility. Furthermore, it also solves the forgotten password problem of righteous users. Multi-key multi-modalities biometric encryption scheme is secure by multiple means as no single user have the complete key to unlock the data, user-keys are derived from their biometric traits those cannot be stolen or hijacked easily by the intruders. User-keys are derived from biometric traits extracting feature templates consequently user personal information is not directly identifiable using user-key therefore user privacy is preserved.

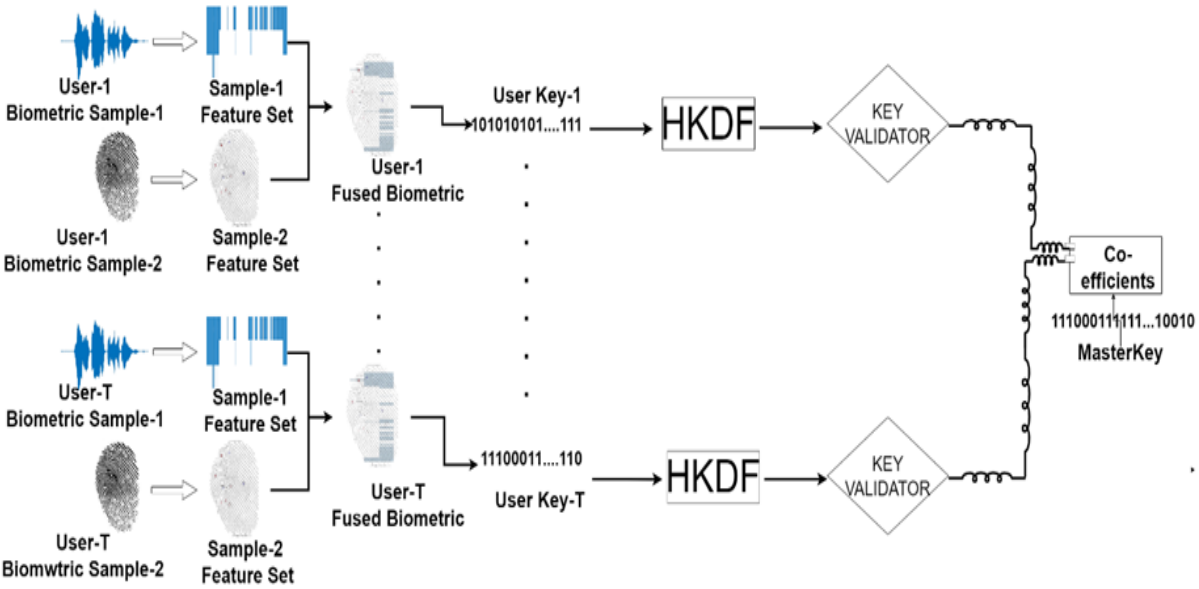


Fig. 2. Multi-key multi-modalities key generation using keys sub-set

Fig. 2., depict the process for on-the-fly re-generation of master-key using threshold number of keys (a subset of the user-keys used to generate master-key). Firstly at-least threshold number users are validated. User-keys are derived for validated users and interpolated using polynomial co-efficient to re-generate the master-key.

3.1.2. HKDF-Based User-Key Generation

The fused multimodal biometric feature vector is transformed into a cryptographic user-key using the Hash-Based Key Derivation Function (HKDF) with SHA-256. The HKDF mechanism ensures fixed-length, irreversible, and cryptographically secure key generation from variable-length biometric feature inputs. The extraction phase of HKDF is defined as:

$$[PRK = HMAC_\{SHA256\}(Salt, F_\{fusion\})]$$

where:

- (PRK) is the pseudo-random key,
- (Salt) represents the deterministic perturbation value applied during feature processing,
- (F_{fusion}) is the fused multimodal biometric feature vector.

Subsequently, the expansion phase derives the final user-key:

$$[UK_i = HKDF(PRK, Info, L)]$$

where:

- (UK_i) denotes the user-key for user (i),
- (Info) represents application-specific context information,
- (L) is the required output key length.

The generated user-key is represented as a fixed-length 256-bit hexadecimal cryptographic key. Since the key is derived from irreversible transformed biometric features rather than raw biometric samples, user privacy is preserved.

3.1.3. Threshold-Based Master-Key Construction

To eliminate centralized trust dependency and improve secure distributed access control, Shamir Secret Sharing is employed for generating the master encryption key from multiple user-keys. A polynomial of degree (t-1) is constructed as:

$$P(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$$

where:

- (a_0) represents the secret master-key,
- (a_1, a_2, ..., a_{t-1}) are randomly selected coefficients,
- (t) denotes the minimum threshold number of valid users required for reconstruction.

Each authorized user receives a share generated as:

$$[S_i = P(x_i)]$$

where:

- (x_i) is the unique identifier associated with user (i),
- (S_i) is the corresponding secret share.

The master-key reconstruction process requires at least (t) valid user shares. Lagrange interpolation is used to reconstruct the secret key as:

$$K=\sum_{i=1}^{t} S_i \prod_{j=1,j\neq i}^{t} \frac{x_j}{x_j-x_i}$$

where:

- (K) denotes the reconstructed master-key,
- (S_i) represents valid user shares.

The reconstructed master-key is finally utilized for AES-based encryption and decryption of business data stored in the cloud environment.

Algorithm 2: Threshold-Based Master-Key Reconstruction

1. Acquire biometric samples from at least (t) authorized users.
2. Preprocess and extract biometric feature vectors.
3. Regenerate corresponding user-keys using HKDF.
4. Validate threshold shares.
5. Apply Lagrange interpolation to reconstruct the master-key.
6. Use the reconstructed master-key for AES decryption of cloud data.

3.1.4. Security and Privacy Preservation

The proposed framework preserves biometric privacy by storing only irreversible transformed feature vectors instead of raw biometric samples. Since the master-key can only be reconstructed when the predefined threshold number of authorized users participate in the reconstruction process, the framework significantly reduces the risks of:

- single-point failure,
- unauthorized access,
- biometric spoofing,
- centralized key compromise.

Furthermore, multimodal biometric fusion improves authentication reliability by combining independent biometric characteristics from fingerprint and audio modalities. Even if one modality becomes partially corrupted or compromised, the remaining modality contributes to maintaining secure authentication and key reconstruction.

3.2. Multi-key multi-modalities key generation using sub-set of user-keys

- AcquireBiometricModalities(): For at-least the decided threshold number of data users: Acquire biometric modalities such as fingerprint and audio modalities
- PreprocessBiometricModalities(): For each acquired biometric modality: Preprocess the biometric modality to prepare it for feature vector extraction

For each data user:

- ExtractFeatureVectors(): Extract feature vectors from the biometric modalities of the data user ensuring privacy preservation.
- ApplyAudioSalting(): Apply audio salting using the same scheme as used to prepare the audio feature key during encryption
- FuseFeatureVectors(): Fuse the feature vectors extracted from different biometric modalities for the data user
- DeriveUserKeys(): Derive user-keys from the fused biometric modalities of the data user using HKDF
- GenerateMasterKey (coefficients, threshold): Get the threshold 't' number of user-keys verified, Generate the master cryptographic key

3.3. Reproducibility and Implementation Details

To improve reproducibility and methodological clarity, all mathematical formulations used in biometric feature extraction, feature fusion, HKDF-based user-key derivation, Shamir Secret Sharing, and Lagrange interpolation have been formally defined using standard equation formatting. All figures have been revised with consistent numbering, captions, and workflow descriptions according to the journal template guidelines. The proposed implementation workflow includes:

- Fingerprint preprocessing and minutiae extraction,
- MFCC-based audio feature extraction,
- Multimodal feature fusion,
- HKDF-SHA256 key derivation,
- Threshold-based master-key reconstruction,
- AES-based cloud data encryption and decryption.

These implementation details are provided to facilitate experimental reproducibility and future comparative evaluation by researchers working in biometric cryptography and cloud security domains.

4. Experiment and Results

The proposed multi-user multi-modal biometric encryption framework was experimentally evaluated using publicly available fingerprint and audio datasets. Fingerprint samples were obtained from the FVC2002 DB1_A dataset, while audio samples were collected from the Mozilla Common Voice (CV-Corpus) dataset. These datasets were selected due to their suitability for multimodal biometric authentication and secure key generation experiments. The fingerprint dataset contains grayscale fingerprint images acquired under controlled acquisition conditions. Fingerprint preprocessing included grayscale conversion, Gaussian smoothing, histogram equalization, normalization, binarization, ridge enhancement, and minutiae extraction. Minutiae feature such as ridge endings and bifurcations were extracted to construct the fingerprint feature vectors. The audio dataset consists of speech recordings from multiple users with varying acoustic characteristics.

Audio preprocessing involved normalization, silence removal, low-pass filtering, resampling, windowing using the Hamming window, dynamic range compression, and MFCC-based feature extraction. In addition to primary MFCC coefficients, first-order and second-order delta coefficients were extracted to capture temporal speech characteristics. For experimentation, multimodal biometric feature vectors were generated by combining fingerprint minutiae features with MFCC-based audio features. Feature normalization and concatenation were performed before deriving cryptographic user-keys using HKDF-SHA256. The generated user-keys were further utilized in Shamir Secret Sharing for threshold-based master-key generation. A threshold configuration of (t)-out-of-(n) users was employed, where at least (t) authorized users were required to reconstruct the master-key for successful decryption. The generated master-key was utilized for AES-based encryption and decryption of cloud-stored business data. The proposed framework was evaluated using multiple security and reliability tests, including:

- Shannon Entropy Test,
- Chi-Square Test,
- Monte Carlo Pi Test,

- Correct Key Decryption Test,
- Incorrect Key Decryption Test,
- Special Character Validation,
- Non-ASCII Character Validation,
- Binary Data Handling Test,
- Large Dataset Encryption/Decryption Test.

These experiments were conducted to evaluate the randomness, reliability, robustness, and threshold-based reconstruction capability of the proposed biometric encryption framework. Experiments were conducted using 100 fingerprint samples and corresponding audio samples from 20 users. AES-256 encryption and SHA-256-based HKDF were implemented using MATLAB R2024a.

4.1. Deterministic Audio Feature Perturbation

To enhance feature diversity and improve resistance against replay and brute-force attacks, a deterministic perturbation mechanism is applied to the extracted MFCC-based audio feature vectors prior to key generation. Unlike conventional password salting used in cryptographic hash functions, the proposed mechanism operates at the biometric feature level and introduces controlled variability into the transformed audio representation. Let the extracted audio feature vector be represented as:

$$[F_{au} = {a_1, a_2, a_3, ..., a_n}]$$

A deterministic perturbation vector (P) is generated using a predefined transformation function:

$$[P = H(UserID || SessionID)]$$

where:

- (H) denotes a SHA-256 based transformation function,
- (UserID) represents the unique user identifier,
- (SessionID) denotes the session-specific parameter.

The perturbed audio feature vector is then computed as:

$$[F_{au}^{*} = F_{au} \oplus P]$$

where:

- (F_{au}^{*}) is the transformed audio feature vector,
- (\oplus) represents feature-level transformation or XOR-based perturbation.

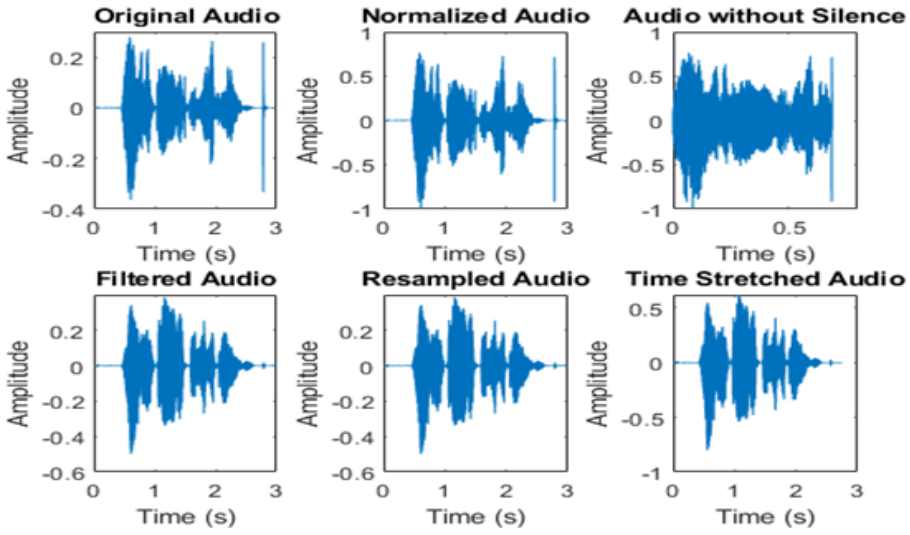


Fig. 3. Workflow of audio preprocessing and MFCC-based feature extraction.

The transformed feature vector is subsequently fused with fingerprint features for cryptographic key generation. Since the perturbation process is deterministic, the same authorized user can regenerate the feature representation during authentication while improving resistance against replay-based attacks and direct feature reconstruction attempts. Firstly, audio is normalized for ensuring consistent amplitude levels using equation 1, then silent segments are removed using an energy threshold using equation 2. Then A low-pass Butterworth filter is applied for eliminating high-frequency noise using equation 3. Afterwards audio is resampled to a standard sampling rate of 44.1 kHz using equation 4. Furthermore, the signal is segmented into overlapping windows, and dynamic range compression is applied for controlling the amplitude variations using equation 5.

Finally, time-stretching is performed to adjust the audio duration without altering its pitch using equation 6.

$$y_{\text{normalized}} = \frac{y}{\max(|y|)} \tag{1}$$

$$y_{\text{without silence}} = y_{\text{normalized}} \quad \text{where} \quad |y_{\text{normalized}}| \geq \text{threshold} \tag{2}$$

$$H(f) = \frac{1}{\sqrt{1 + \left(\frac{f}{f_c}\right)^{2n}}} \tag{3}$$

$$y_{\text{resampled}} = resample\left(y, F_{\text{new}}, F_{\text{original}}\right) \tag{4}$$

$$y_{\text{compressed}} = \frac{y_{\text{resampled}}}{max\left(\left|y_{\text{resampled}}\right|\right)}. \tag{5}$$

$$y_{\text{stretched}} = resample\left(y_{\text{compressed}}, P, Q\right) \tag{6}$$

Fingerprint images are pre-processed as depicted in Figure 4, images are resized and converted to grayscale further images are smoothen using 2-D Gaussian smoothing kernel with standard deviation of 0.5, next images are equalized using histogram equalization, thereafter images normalized to the range [0,1] using Otsu's method, global threshold is used to minimize the infraclass variance, next images are binarized and enhanced, images masks are generated and minutiae are identification such as termination, bifurcation, crossing and dot, in last, false minutiae are identified and removed.

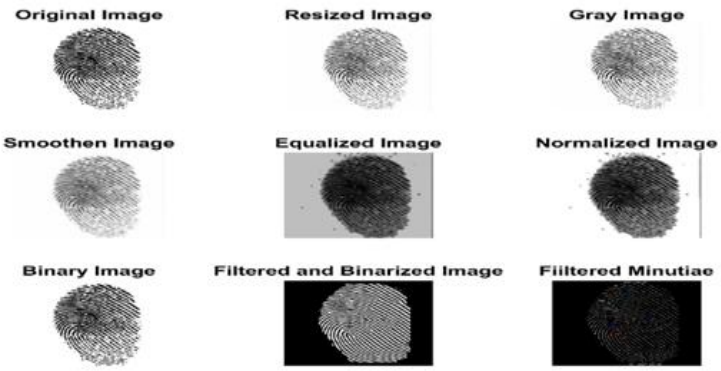


Fig. 4. Fingerprint image pre-processing

Firstly, the image is converted to grayscale. Gaussian smoothing is then applied to reduce noise and smooth the image using equation 7, then histogram equalization is applied to enhance the contrast and improve details visibility using equation 8. The image is normalized to the range [0, 1] for standardizing its intensity values. Afterwards, global thresholding is performed to convert the image into a binary format using equation 9.

$$I_{\text{smoothed}} = G_\sigma * I \tag{7}$$

$$I_{\text{equalized}} = T(I) \tag{8}$$

$$I_binary = \begin{cases} 1 & if\ I_equalized >= threshold \\ 0 & otherwise \end{cases} \tag{9}$$

After pre-processing the audio samples and fingerprint images, privacy preserved feature extraction is performed such that user identity cannot be determined using the feature vectors. Pre-processed fingerprint image is used for extracting minutiae (ridge endings and bifurcations) by following the sequence of steps, Firstly, image is converted to grayscale and enhanced by removing noise. Then unnecessary background regions are identified and removed and masking is applied to focus on the fingerprint areas, and detects the core point of the fingerprint. Minutiae are extracted by analysing ridge patterns, and then false minutiae are filtered out based on proximity and ridge continuity. Furthermore, the delta points are also identified and ridge count is computed between minutiae pairs.

The MATLAB "mfcc" function is used on pre-processed audio. Which internally divides the signal into short overlapping frames, applies a Hamming window, and computes the Short-Time Fourier Transform (STFT) to get the magnitude spectrum. The spectrum is mapped to the Mel scale using a Mel filter bank and the logarithm of the filter bank energies is calculated. Further, The Discrete Cosine Transform (DCT) is applied to extract the Mel-Frequency Cepstral Coefficients (MFCCs) using equation 10, where first 13 coefficients retained as primary features. To capture temporal dynamics the first-order (delta) and second-order (delta-delta) derivatives of the MFCCs are computed by applying a weighted difference between consecutive frames, where delta features are calculated using equation 11(21) (21). The MFCCs, delta MFCCs, and delta-delta MFCCs are concatenated into a single feature matrix. Which is normalized to have zero mean and unit variance for consistency. By following the above listed process both spectral and temporal characteristic of audio sample are captured.

$$\text{MFCCs} = DCT\left(log\left(\text{MelFilterbank}\left(STFT\left(y_{\text{preprocessed}}\right)\right)\right)\right) \tag{10}$$

$$\Delta(t) = \frac{\sum_{n=1}^{N} n \cdot \left(c(t+n) - c(t-n)\right)}{2 \cdot \sum_{n=1}^{N} n^2} \tag{11}$$

A Deterministic Audio Salt is generated using equation 12, Audio features vector is merged with a deterministic random salt to prevent from the brute force attack. Features are extracted from salted audio. Fingerprint features and audio features are normalized using equation 13(13), normalized audio and fingerprint features are concatenated. To derive the User-key from the concatenated features, a Hash-Based Key Derivation Function (HKDF) is used where HMAC-SHA256 (Hash-Based Message Authentication Code with SHA-256) algorithm is applied to the concatenated features to generate a fixed-length key of 64 hexadecimal characters using equation 14.

$$\text{Salt} = H(\text{Feature}_1 | \text{Feature}_2 | \cdots | \text{Feature}_N | Metadata) \tag{12}$$

$$\text{Features}_{\text{normalized}} = \frac{\text{Features} - \mu}{\sigma} \tag{13}$$

$$\text{User-key} = \text{HKDF (Concatenated Features, Salt, Info)} \tag{14}$$

To time and refine the multi-modality key several tests are conducted in detail. Initially, Shannon Entropy Test is used to determine the randomness of the key for understanding whether key has enough amount of randomness in it or not.

Key Testing Results: Fused_Key+HKDFwithAudioPCA

Test Case	Result
Shannon Entropy Test	Success
Chi-Square Test	Success
Monte Carlo Pi Test	Failure
Decryption Test	Success
Incorrect Key Decryption Test	Success
Special Characters Test	Success
Long Message Test	Success
Binary Data Test	Success
Large Dataset Test	Success
Non-ASCII Characters Test	Success

MATLAB R2024a Author: Sahil Rampal

Fig. 5. Fused Key using PCA +HKDF key Performance tests result

The Chi-Square test used to determine the suitability of the key data pattern in possessing the expected statistical properties. The Monte Carlo Pi Test is used for testing whether the key is random or not as easy ways to guarantee that the keys are random. The Decryption Test is conducted to ensure that the decryption process restores the contained information with accuracy. Other tests conducted include the Incorrect Key Decryption Test where the objective is to make sure that the system fails safely if the wrong key is used to decrypt information. Special Characters Test is carried out to confirm that messages containing special characters decrypt to the original message. Non-ASCII Characters Test is used to check whether the message containing non-ASCII characters decrypt to the original message. Moreover, Long Message Test, Binary Data Test, and Large Dataset Test are also conducted to test the system for its ability to handle large inputs. Figure 5 shows the results of various test conducted for the key where PCA is applied to audio feature set before concatenating with fingerprint and Key derived from concatenated features set using HKDF (Hash based key derivation function which uses hash-based message authentication code).

Collectively these tests ascertain the reliability, security, and the effectiveness of the encryption key in adverse conditions. Only test failed for multi-modality key with HKDF is Monte Carlo Pi Test which indicates key randomness, latterly with extermination its learnt that PCA applied on audio for dimensionality reduction effected the key randomness. The fused key is regenerated by directly selecting first 13 prominent MFCCs derived from the audio, combining them with first-order and second-order delta features to form the audio feature vector. This vector is then concatenated with the fingerprint feature vector, and HKDF is applied to derive the encryption key Figure 6 shows the results of various test, this time key successfully cleared all the tests including Monte Carlo Pi Test.

Key Testing Results: Fused_Key+HKDF

Test Case	Result
Shannon Entropy Test	Success
Chi-Square Test	Success
Monte Carlo Pi Test	Success
Decryption Test	Success
Incorrect Key Decryption Test	Success
Special Characters Test	Success
Long Message Test	Success
Binary Data Test	Success
Large Dataset Test	Success
Non-ASCII Characters Test	Success

MATLAB R2024a Author: Sahil Rampal

Fig. 1. FusedKey+HKDF Performance tests result

Subsequently master-key is generated using polynomial for secret sharing (Shamir Secret Sharing) approach where $P(x)$ of degree k−1is defined using equation 15 and shares are generated using equation 16. User-keys are combined while ensuring combined key fits within a fixed range using equation 17. A Master-Key (multi-key multi modalities biometric key) is generated from the combined-key using SHA256 hashing method using equation 18. AES symmetric-key encryption is performed with the generated master key to encrypt the data. Encrypted data uploaded to cloud space for storage and later retrieval.

$$P(x)=s+r_1x+r_2x^2+\cdots+r_{k-1}x^{k-1} \tag{15}$$

$$d(i)=P(i) \tag{16}$$

$$\text{combined_key} = \text{mod}\left(\text{numeric_codes_sum}, 10^{10}\right) \tag{17}$$

$$\text{master_key}=\text{SHA-256}(\text{combined_key}) \tag{18}$$

To decrypt the data master-key is re-generated by performing Lagrange Interpolation with k or more shares (validated user-keys) to reconstruct the secret from a subset of shares using equation 19. Explicit interpolation coefficients are not needed because the Lagrange interpolation formula dynamically computes the necessary terms using the share indices. Lagrange basis polynomials are constructed on-the-fly for each share j using equation 12, and interpolation performed to generate the share using equation 21. When the secret is generated master-key is reconstructed with SHA256 hashing.

$$secret = \Sigma_{j=1}^{t} y_j \cdot \Pi_{\substack{i=1, \\ i\neq j}}^{t} \frac{x}{x_i - x_j} \ (mod\ p) \tag{19}$$

$$l_{i(x)} = \prod_{\substack{j=0 \\ ,j\neq i}}^{n} \frac{(x - x_j)}{(x_i - x_j)} \tag{20}$$

$$P(x) = \sum_{i=0}^{t} y_i \cdot l_{i(x)} \tag{21}$$

AES symmetric encryption utilizes the re-constructed master-key to decrypt the data. Data is decrypted successfully after downloading from cloud. further as per scheme requirement less than threshold user-keys are not generating the master key. consequently, data is not decrypted with less than the threshold number of user-keys. Mater-Key (Multi-Key Multi-Modality Biometric Encryption Key) performance is evaluated using the standard tests to test the encryption key performance and reliability. Master-Key successfully cleared the performance and security related tests. Fig. 7. shows the results of various tests conducted for testing the performance and reliability of the master-key. Master key cleared Shannon Entropy Test which ensure the randomness of the key. Master-Key cleared Chi-Square Test which ensured key data pattern exhibit expected statistical properties. The Monte Carlo Pi Test cleared by master-key ensured the randomness of the key generation process. Various Decryption Tests conducted to ensure that the decryption process correctly decrypt the data with accuracy for Special Characters, Non-ASCII Characters Long Message, Binary Data and Large Datasets. Incorrect Key Decryption Test is also successfully cleared by master key where the objective is to make sure that the system fails safely if the wrong key is used to decrypt information.

Key Testing Results: Master_Key

Test Case	Result
Shannon Entropy Test	Success
Chi-Square Test	Success
Monte Carlo Pi Test	Success
Decryption Test	Success
Incorrect Key Decryption Test	Success
Special Characters Test	Success
Long Message Test	Success
Binary Data Test	Success
Large Dataset Test	Success
Non-ASCII Characters Test	Success

MATLAB R2024a
Author: Sahil Rampal

Fig. 7. Master-Key performance tests results

As per the business requirement and level of data superiority this encryption scheme can be easily extended to further enhance the security of the system by checking the liveliness of samples to avoid the use of stored biometric or maliciously obtained biometric samples. To further increase the system security, origin of the download data request can be verified, to ensure that business data can be accessed only from the business premises. Which in terms save the data to be accessed by the employee from outside of the business premises.

4.2. Single Party Business

Single party business using cloud for data storage can apply multi-key multi-modalities biometric encryption at the last network device, before transmitting the data to any other network or to cloud space. Which in terms has its own advantages, indeed it removes the security challenges of data-in-transit and data stored at cloud.

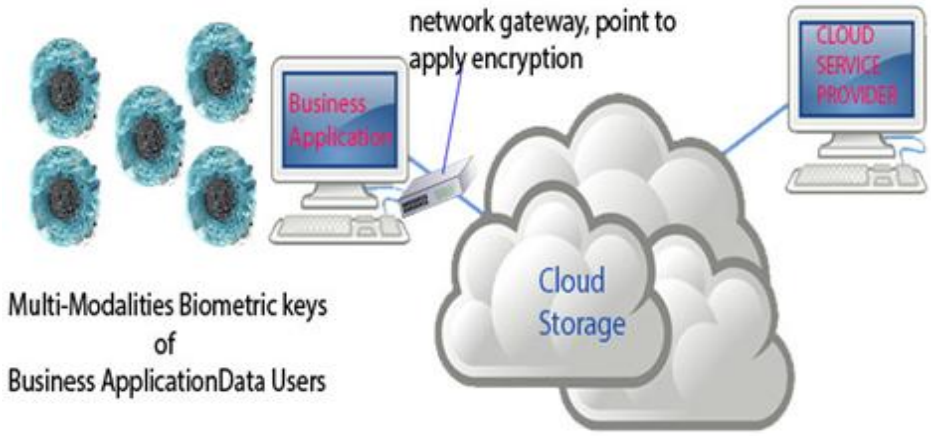


Fig. 8. Multi-Key Multi-modalities biometric encryption for Single Business Application data users

Fig. 8. explains the approach for encrypting business application data using multi-key multi-modalities biometric encryption. In this approach all the data users will give their biometric samples for encrypting business data with multi-key multi-modalities biometric encryption key. To store any business data at cloud space, data is encrypted using the final master key and encrypted using the symmetric key cryptography with multiple re-encryption scheme such as RSA.

4.3. Multi-party Businesses

Multi-party businesses security requirement is little different than single business. In case of multi-party businesses using cloud for data storage, having their own networks they can create multi keys, one with respect to each location/business. Biometric encryption keys of their users will be utilized to generate master encryption key. They may use a single key or generate a key per business and share with other business parties' second case is more secure than the other. User of any business can access the data as per there level of access on the requested data.

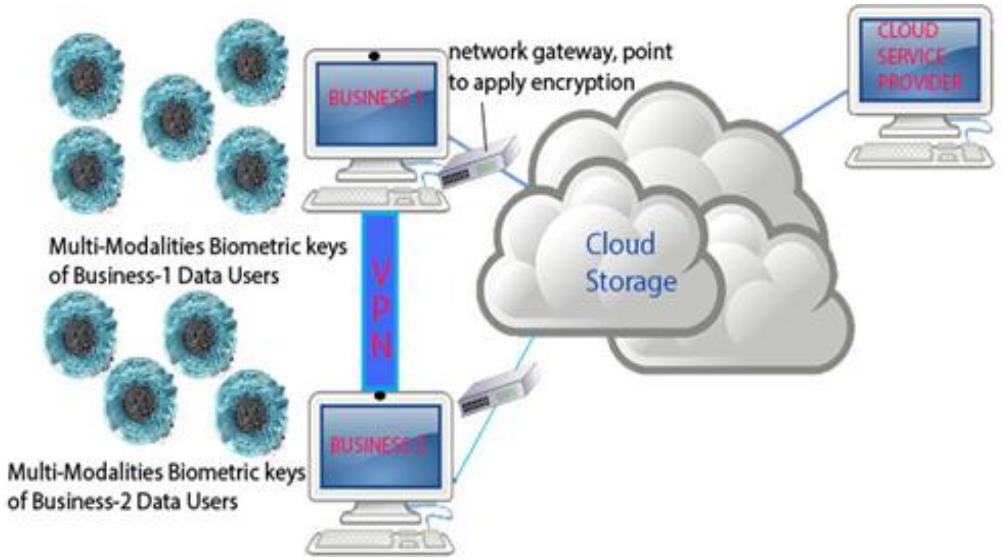


Fig. 9. Multi-Key Multi-modalities biometric encryption for multiple businesses exchanging data using cloud.

Fig. 9. explain the process for multiple business sharing their encryption keys with other business parties, businesses can communicate using the virtual private network to save from unauthorized access or hijacking of the encryption keys, VPN will also ensure that no one other than users of allowed networks can request for decrypted data. Furthermore, cloud service provider cannot access or modify the data stored in the public cloud as data is encrypted with business encryption key but not provided by cloud provider. This approach will save the businesses from unauthorized access by business employees as well. As they were unable to access the decrypted data outside the network, if the cloud provider is malicious and provide the access for encrypted data to any employee then also, they do not have the master key as single sub key is not enough to generate the master key, resultant they will not get access to the decrypted data.

Due to use of multi-key encryption all the involved user can access the data once properly authorized. This scheme can easily be implemented at the departments level. Where each department require generating its own key and sharing with other department for sharing data with the other departments of business. This security scheme is secure by the means of hiding valuable information from the hackers. Our approach of securing cloud data of business applications is much safer as cloud service provider does not know the encryption key used to secure the data. Nevertheless, to make the system more robust, high similarity index should be used to consider the matches. Further the cloud security can be enhanced at the level of cloud service provider by adding security captcha, setting number of wrong attempts, and enabling 2-step authentication, etc. This will further raise the level of the security to some more extent. Locking the account after of minimum wrong attempts can help in neutralize the brute force attack. Security of cloud data is the responsibility of both cloud users and cloud service provider; they need to works collectively to improve the cloud security.

4.4. Security Evaluation Discussion

The proposed framework was evaluated using multiple statistical randomness and decryption reliability tests to examine the practical robustness of the generated biometric encryption keys. Shannon Entropy, Chi-Square, and Monte Carlo Pi tests were utilized to assess the randomness characteristics of the generated cryptographic keys. In addition, decryption validation tests were conducted to verify the correctness and reliability of the threshold-based master-key reconstruction process. Although statistical randomness tests provide useful indicators regarding key unpredictability and distribution properties, such tests alone do not constitute formal cryptographic security proofs. The security of the proposed framework primarily relies on the combined strength of:

- Multimodal biometric feature fusion,
- HKDF-SHA256-based key derivation,
- Threshold-based Shamir Secret Sharing reconstruction,
- AES symmetric encryption.

The threshold-based reconstruction mechanism improves resistance against single-point failure because the master-key cannot be regenerated unless the predefined minimum number of valid user-keys are available. Furthermore, the use of irreversible transformed biometric features enhances privacy preservation and reduces the risk of direct biometric reconstruction. The proposed framework is intended as a practical secure access-control and cloud data protection mechanism rather than a formally verified cryptographic protocol. Future work may include formal cryptographic security analysis, adversarial threat modeling, computational complexity evaluation, and resistance analysis against replay, spoofing, and side-channel attacks.

4.5. Comparative Analysis with Existing Approaches

A comparative analysis was conducted to evaluate the proposed framework against existing biometric encryption and cloud security approaches. Table X summarizes the major characteristics and limitations of representative methods from the literature. Existing uni-biometric authentication systems primarily rely on a single biometric modality, making them vulnerable to biometric variability, spoofing attacks, and single-point failure. Similarly, conventional cloud encryption frameworks often depend on centralized key management mechanisms, increasing the risk of unauthorized access if the encryption key is compromised. Recent studies incorporating blockchain and multi-factor authentication improve decentralized access control and auditability; however, many of these approaches introduce increased computational overhead and do not integrate threshold-based biometric cryptographic reconstruction. Moreover, several existing methods focus primarily on authentication rather than secure distributed key generation for cloud data protection. In contrast, the proposed framework combines:

- Multimodal biometric fusion using fingerprint and audio features,
- HKDF-based cryptographic user-key generation,
- Threshold-based Shamir secret sharing reconstruction,
- Distributed trust-based cloud access control.

The threshold-based reconstruction mechanism ensures that the master-key cannot be regenerated unless the minimum predefined number of authorized users participate in the reconstruction process. This significantly reduces the risk of single-user compromise and unauthorized cloud access.

Table 1. Comparative Analysis of Existing Biometric Encryption and Cloud Security Approaches with the Proposed Multi-User Multi-Modal Threshold-Based Framework

Reference / Method	Biometric Type	Multi-Modal Authentication	Threshold-Based Access Control	Distributed Trust Mechanism	Cloud Data Protection	Resistance to Single-Point Failure
Jagadiswary & Saraswady [21]	Fingerprint + Face	Yes	No	No	Limited	No
Hammad et al. [22]	ECG + Fingerprint	Yes	No	No	Limited	Partial
Barman et al. [17]	Crypto-Biometric Credentials	Partial	No	Multi-Server Support	Moderate	Partial
Ramya et al. [14]	Multi-Factor Authentication	No	No	No	Yes	No
Nalluri et al. [7]	Multi-Factor Authentication	Partial	Partial	Blockchain-Based	Yes	Moderate
Bharot et al. [16]	Hybrid Cryptographic Framework	No	No	Multi-Cloud Support	Yes	Partial
Hammed et al. [6]	Biometric Authentication	No	No	Decentralized Network	Yes	Partial
Proposed Framework	Fingerprint + Audio	Yes	Yes	Yes	Yes	Yes

Furthermore, unlike conventional password-based or centralized encryption systems, the proposed framework utilizes irreversible transformed biometric feature vectors, thereby improving privacy preservation and reducing dependency on stored static credentials.

5. Conclusion and Future Scope

Cloud computing provides scalable and cost-effective infrastructure for modern businesses; however, ensuring secure access to sensitive cloud-stored data remains a critical challenge. This paper proposed a multi-user multi-modal biometric encryption framework integrated with threshold-based master-key reconstruction for enhancing cloud data security and distributed access control. The proposed approach combines fingerprint and audio biometric modalities with HKDF-based cryptographic key generation and Shamir Secret Sharing to establish secure and privacy-preserving cloud data protection. Experimental evaluation using fingerprint and audio datasets demonstrated that the generated biometric encryption keys satisfied statistical randomness and decryption reliability tests, including Shannon Entropy, Chi-Square, Monte Carlo Pi, and threshold-based reconstruction validation. The proposed framework effectively reduces single-point failure risk by requiring participation of a predefined threshold number of authorized users for successful master-key reconstruction.

Although the obtained results demonstrate the practical feasibility and robustness of the proposed framework, the current work represents a preliminary experimental study rather than a formally verified cryptographic protocol. The conducted statistical evaluations provide empirical validation of key randomness and reconstruction reliability; however, formal security proofs, adversarial threat modeling, computational complexity analysis, and resistance evaluation against spoofing and side-channel attacks remain important directions for future research. In future work, the proposed framework

may be extended toward lightweight privacy-preserving cloud security architectures, blockchain-integrated distributed access systems, and homomorphic encryption-based secure cloud computation environments.

All the Declarations and Statements

Author Contributions Statement

Sahil Rampal – formal analysis, methodology, resources, software, visualization, original draft
Manmohan Sharma – investigation, visualization, original draft, review, and editing
Parul Khurana – validation, original draft, review, and editing
Mukesh Kumar – validation, original draft, review, and editing

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

The authors declare that no funding was received for this study.

Data Availability Statement

The data used in this study are available from the corresponding author upon reasonable request.

Ethical Declarations

This study did not involve human participants or animals. Therefore, ethical approval was not required.

Acknowledgments

The authors wish to thank Hanoi National University of Education.

Declaration of Generative AI in Scholarly Writing

During the preparation of this manuscript, the author(s) used OpenAI to improve the clarity and readability of selected paragraphs. The generated text was edited and revised as needed, and all content remains the responsibility of the author(s). No AI tool is listed as an author.

Abbreviations

The following abbreviations are used in this manuscript:

NIST - National Institute of Standard and Technology
HKDF - Hash-Based Key Derivation Function
MFCCs - Mel-frequency cepstral coefficients
STFT - Short-Time Fourier Transform
PCA - Principal Component Analysis
DCT - Discrete Cosine Transform
CSA - Cloud Security Alliance

Appendix A\B\C…, with appendix tile

None.

References

[1] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,” 2011.
[2] Sinha, K., Aldosary, S., Aly, M. H., & El-Shafai, W. (2025). Enhancing Cloud Data Security Through Functional-Based Stream Cipher and Attribute-Based Access Control with Multiparty Authorization. Traitement du Signal, 42(2), 915.

[3] Garigipati, N., Srithar, S., & Krishna Reddy, V. (2026). An efficient poly-quantum integrity key generation based multi-user access control encryption and decryption framework for homogeneous and heterogeneous cloud EHR databases. Information Security Journal: A Global Perspective, 35(1), 168-188.
[4] Y. Chen, V. Paxson, and R. H. Katz, "What's New About Cloud Computing Security?," EECS Department, University of California, Berkeley, 2010. [Online]. Available: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html
[5] Murala, D., & Thammireddy, K. (2024). An Efficient Multi-user Integrity and Multi-level Attribute Encryption and decryption framework for audio block-chain communication systems. Frontiers in Health Informatics, 13(3).
[6] Hammed, S. S., Pavalarajan, S., Preethi, C., & Haripriya, K. (2026). Multi-level Cloud Security with Encryption Using Biometric Authentication in Decentralized Network. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 1-23.
[7] Nalluri, S., Veeravalli, S. D., Srinath, S., Mrumudhe, S. T. A., & Harit, V. (2025, June). Blockchain-Based Multi-Factor Access Control for Preserving Privacy in Cloud Storage of Medical Records. In 2025 International Conference on Intelligent Computing and Knowledge Extraction (ICICKE) (pp. 1-6). IEEE.
[8] The Notorious Nine Cloud Computing Top Threats in 2013, Online link: https://Cloudsecurityalliance.Org/Artifacts/The-Notorious-Nine-Cloud-Computing-Top-Threats-In-2013, Access date: 24/10/2024
[9] Security guidance for critical areas of focus in cloud computing v3.0, Online link: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, Access date: 24/10/2024
[10] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Online link: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, Access date: 24/10/2024
[11] Security Guidance For Critical Areas of Focus in Cloud Computing, Online link: https://cloudsecurityalliance.org, Access date: 24/10/2024
[12] Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Online link: https://cloudsecurityalliance.org/artifacts/security-guidance-v4, Access date: 24/10/2024
[13] Biometrics-Technologies For Highly Secure Personal Authentication, Online link: https://www.nist.gov/publications/biometrics-technologies-highly-secure-personal-authentication, Access date: 24/10/2024
[14] Ramya, M., Tamilvizhi, T., & Navaneethakrishnan, S. R. (2025, September). Enhancing cloud security with multi-factor authentication and optimized encryption algorithm. In 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1033-1039). IEEE.Ross and A. Jain, "Information fusion in biometrics," Pattern Recognit Lett, vol. 24, no. 13, pp. 2115–2125, Mar. 2003, doi: 10.1016/S0167-8655(03)00079-5.
[15] Santoso, A., Huda, S., Kodera, Y., & Nogami, Y. (2025). Facial Privacy Protection with Dynamic Multi-User Access Control for Online Photo Platforms. Future Internet, 17(3), 124.
[16] Bharot, N., Mehta, N., Breslin, J. G., & Verma, P. (2025). Cloudlock: secure data sharing using a hybrid cryptosystem in multi-cloud data storage. Cluster Computing, 28(7), 464.
[17] Barman, S., Chattopadhyay, S., & Samanta, D. (2024). Toward design a secure protocol for updating remotely stored credentials of a crypto-biometric framework for multi-server environment. Security and Privacy, 7(1), e339.
[18] Adeoye, S., & Adams, R. (2024). IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach towards a trustworthy cloud computing. Cogn. J, 4(10), 183-209.
[19] Cai, J., Zhao, X., Li, D., Li, H., & Fan, K. (2025). Efficient and expressive public key authenticated encryption with keyword search in multi-user scenarios. arXiv preprint arXiv:2503.16828.
[20] Neela, K. L. (2024). DSDOS Cloud: A Decentralized Secure Data Outsourcing System With Hybrid Encryption, Blockchain Smart Contract-Based Access Control, and Hash Authentication Codes for Cloud Security. Transactions on Emerging Telecommunications Technologies, 35(11), e70016.
[21] D. Jagadiswary and D. Saraswady, "Biometric Authentication Using Fused Multimodal Biometric," Procedia Comput Sci, vol. 85, pp. 109–116, 2016, doi: 10.1016/j.procs.2016.05.187.
[22] M. Hammad, Y. Liu, and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint," IEEE Access, vol. 7, pp. 26527–26542, 2019, doi: 10.1109/ACCESS.2018.2886573.

Authors' Profiles



Dr. Sahil Rampal is an Associate Professor at the School of Computer Applications, Lovely Professional University, Punjab, India, with over 18 years of experience in teaching and research. He holds a B.Sc. in Information Technology (2005) from Guru Nanak Dev University, an MCA (2008) from Punjabi University, Patiala, and a Ph.D. in Computer Applications (2025) from Lovely Professional University. His research focuses on Data Security, Biometric Encryption, Multi-Modality Fusion, and Cryptography. He has published research in reputed journals and international conferences and actively contributes to advancing secure computing solutions.



Dr. Manmohan Sharma is Professor in the School of Computer Applications at Lovely Professional University with over 26 years of experience in academics, research, and administration. He received his Ph.D. in Wireless Mobile Networks from Dr. B.R. Ambedkar University in 2014. His research interests include Wireless Mobile Networks, Mobile Cloud Computing, Data Science, and Machine Learning. He has authored/co-authored 68+ research papers, holds 4 patents and 3 copyrights, and has successfully supervised 10 Ph.D. and 3 M.Phil. scholars. He is actively associated with professional bodies including IEEE, Association for Computing Machinery, and Computer Society of India.. He can be contacted via email at manmohan.sharma71@gmail.com



Dr. Parul Khurana is Professor in the Department of Computer Science & Applications, Sharda School of Computing Science & Engineering, Sharda University with a strong academic and research background in the areas of Data Science, Informetric, Gamification, Cloud Computing, and emerging computing technologies. He is an active researcher with a growing national and international research footprint reflected through his scholarly publications and citation impact. He can be contacted via email at parul.khurana@sharda.ac.in



Dr. Mukesh Kumar is an Associate Professor at Advanced Centre of Research & Innovation (ACRI), CGC University Mohali-140307, Punjab, India, and an Adjunct Associate Professor in the Faculty of Law, Solar University Oman. He holds a Ph.D. in Computer Science from Himachal Pradesh University, Shimla, where he specialized in designing ensemble and hybridized data mining techniques for analyzing academic performance. With over 15 years of experience in academia, Dr. Kumar has held various teaching positions, including Assistant Professor at Lovely Professional University and Chitkara University. He has contributed to various international conferences and holds intellectual property rights for several innovations.

How to cite this paper

Sahil Rampal, Manmohan Sharma, Parul Khurana, Mukesh Kumar, "Enhancing Cloud Storage Security Using Multi-User Biometric Encryption with Threshold Access Control", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.3, pp. 142-159, 2026. DOI:10.5815/ijwmt.2026.03.10