Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2650

A framework for secure cloud operations via homomorphic encryption and euclidean biometric matching

Ritik Mittal [§]
Pradeep Kumar [†]
Kuntal Gaur *
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

In the evolving landscape of secure cloud automation, this paper introduces a novel AI-driven framework that integrates homomorphic encryption (HE), facial biometric authentication, and encrypted voice-command processing to achieve intelligent, privacy-preserving cloud resource management. Unlike prior models that depend on plaintext computation or modular scripts, our system performs encrypted biometric matching and command parsing, orchestrating cloud operations through secure tokens generated in the encrypted domain. This architecture, built atop AWS services such as EC2, Lambda, IAM, and Polly, ensures cryptographic isolation and integrity of sensitive workflows. Experimental results demonstrate authentication accuracy of 96.2%, command latency under 2.8 seconds, and significant performance gains over traditional interfaces, with zero leakage under chosen-ciphertext attack simulations. The proposed framework sets a new benchmark for secure, encrypted, and intelligent cloud management.

Subject Classification: *Primary 94A60, Secondary 68M14.*

Keywords: *Homomorphic encryption, Secure AI, Facial biometrics, Voice command, Cloud automation, Cryptographic NLP, AWS security, Zero-knowledge protocols, Privacy preservation.*

[§] *E-mail:* `ritik.2410200002@muj.manipal.edu`
[†] *E-mail:* `Pradeep.kumar@jaipur.manipal.edu`
* *E-mail:* `Kuntal.gaur@jaipur.manipal.edu (Corresponding Author)`

1. Introduction

Cloud computing has evolved into the backbone of modern digital services, supporting enterprise infrastructures, IoT deployments, and critical applications across healthcare, finance, and defense. However, as reliance on cloud environments deepens, ensuring secure, user-friendly, and privacy-preserving interaction becomes vital. Traditional methods, such as access via key pairs or static credentials, remain vulnerable to interception, misuse, or human error. These limitations have increased the exploration of biometrics and natural language interfaces to simplify and strengthen the authentication mechanisms.

Facial recognition and voice interaction are natural and effortless modes of authentication primarily when it is designed for real-time operations. These modalities also present multiple different types of privacy risks facial templates and voice features, once they are exposed. These are hard to revoke or regenerate. To tackle this, the researchers have more looked to homomorphic encryption (HE) as a solution which enables sensitive computations like matching and verification to be performed directly on encrypted data. This makes sure that even if the computation environment is breached, the personal data is still protected.

Recent work has shown the suitability of combining HE with biometric authentication [1][2][3] and natural language processing [4][5] [11][12]. Furthermore, new access control protocols and secure automation schemes have arisen in response to increasing demands for dynamic, scalable, and role-based cloud environments [6][7]. These advances provides a chance to consider highly safe and secure cloud orchestration by using a single framework which integrates biometric input, voice interfaces, and cryptographic processing.

This framework combines an improved system that includes real-time facial and voice recognition into cloud services. Which makes sure that every interaction is combined with secure, encrypted tokens.

Unlike past solutions which either focus mainly on usability or on privacy. Our framework combines both the things with offering a scalable and modular system deployable in public cloud platform such as AWS.

2. Related Work

Gentry's work on fully homomorphic encryption [1] introduced the potential of performing computations directly on encrypted data. Since

then, various partially and fully homomorphic encryption schemes have optimized encrypted computations for practical applications [8][9].

In biometric authentication, The Local Binary Pattern Histogram (LBPH) approach was developed [10], which has been widely adopted for real-time facial recognition due to its efficiency on low-resource devices. Troncoso-Pastoriza, Gonzalez-Jimenez, and Perez-Gonzalez [2] demonstrated that LBPH templates could be securely matched using Paillier encryption, enabling encrypted domain verification.

Voice recognition and command parsing have seen rapid development with the advent of deep learning models. End-to-end deep neural network based acoustic modeling has demonstrated high accuracy in speech recognition tasks [4]. However, most systems operate in the plaintext domain, raising privacy concerns. Nautsch explored secure voice interfaces leveraging homomorphic encryption [5].

On the cloud orchestration front, AWS Boto3 and tools like Terraform and Ansible have streamlined infrastructure management but lack built-in support for biometric and voice-activated secure control. Halder and Newe [6] validated the integration of HE for secure IoT and biometric workflows.

This paper builds on these foundations to present a complete, end-to-end system that performs cloud operations only after privacy-preserving, encrypted authentication [11][12].

3. System Architecture

The proposed system is structured into three modular components that work in unison to enable secure and intelligent cloud orchestration. The FaceAuth Module captures facial images, extracts features using the Local Binary Pattern Histogram (LBPH) method, and encrypts them using Paillier encryption to ensure privacy during matching. The VoiceCommand Module processes spoken input by extracting Mel-Frequency Cepstral Coefficients (MFCC) features, which are similarly encrypted prior to semantic analysis. Finally, the HECloud Module utilizes AWS services such as Boto3 and Lambda to execute cloud operations, which are triggered only upon successful multi-modal biometric authentication and validation of encrypted command tokens.

Modules interact through an event-driven controller. Encrypted features are matched homomorphically, and control tokens are generated based on multi-modal inputs.

4. Methodology

This section outlines both the original prototype and the proposed cryptographic enhancements in exhaustive technical depth, ensuring clarity, reproducibility, and rigor.

4.1 *Functional Prototype Implementation:*

The baseline system was developed in Python using OpenCV, pyttsx3, speech_recognition, and AWS Boto3 libraries. It comprises three primary modules:

4.1.1 Facial Recognition with LBPH and OpenCV:

Facial images are captured in real-time using a webcam and localized through a Haar cascade classifier to detect facial regions. These images are then converted to grayscale, resized to 130×100 pixels, and processed with histogram equalization to normalize lighting conditions. From the preprocessed images, Local Binary Pattern Histogram (LBPH) features are computed and stored for each user. The system trains user-specific LBPH models on the collected dataset, serializes them, and maintains them for future comparisons. During operation, a recognition module matches incoming facial inputs against the stored models using a confidence threshold of 75% to ensure reliable authentication.

4.1.2 Voice Command Interface:

Voice input is captured using a high-sensitivity microphone and processed through the Google Speech API to convert speech into text, while text-to-speech responses are provided using the pyttsx3 engine. The system supports a range of cloud management commands, including EC2 instance creation and termination, EBS volume management, IAM user creation, S3 bucket and file operations, and email broadcasting via AWS SES. Robust error-handling mechanisms are integrated to make sure proper fallback and continued operation in cases of command misrecognition or processing errors.

4.1.3 Cloud Automation via Boto3:

Cloud resources which are managed by Python scripts which is integrated with the Boto3 library. It enables seamless automation of multiple AWS services. This system supports EC2 instance operations wirh using create_instances() and terminate_instances(), IAM user

provisioning by policy-based controls, and S3 for bucket and file management. Also, it uses Amazon Polly service for multilingual voice synthesis and AWS SES for sending templated email campaigns. Which ensures a fully automated and voice-activated cloud orchestration workflow.

4.2 *Cryptographic Enhancement with Homomorphic Encryption:*

To mitigate privacy issues in the baseline system, the framework is enhanced with a Paillier-based encrypted processing pipeline.

4.2.1 Preprocessing:

Facial images are further normalized to ensure uniform vector scaling, enhancing consistency across biometric samples, while voice signals undergo spectral subtraction and Voice Activity Detection (VAD) to isolate meaningful speech segments and eliminate background noise, thereby improving the accuracy and reliability of subsequent encrypted feature extraction.

4.2.2 Feature Extraction and Encryption:

MFCC features from voice input are encrypted similarly to maintain a consistent privacy layer. Each LBPH histogram feature x_i is encrypted:

$$E(x_i) = g^{x_i} * r^n \ \ (mod\, n^2) \tag{1}$$

where g is the generator, r is a random nonce, and n is the Paillier modulus.

4.2.3 Encrypted Matching and Verification:

Biometric comparison uses homomorphic Euclidean distance computation:

$$E(\| x - x' \|^2) = E(\Sigma_{i=1}^{d} x_i^2) * E(\Sigma_{i=1}^{d} x_i'^2) * E(-2\Sigma_{i=1}^{d} x_i x_i') \tag{2}$$

Matching is performed entirely in the encrypted domain, ensuring that plaintext biometric data is never revealed or stored. After successful verification, a secure token is generated:

$$T = E(SHA256(x_f + x_v + K))(\mathrm{mod}\, n^2) \tag{3}$$

where x_f and x_v are encrypted facial and voice features, and K is a system-generated nonce. The encrypted token triggers AWS Lambda functions for cloud orchestration.

4.2.4 Security Logging and Role Management:

Facial images are normalized to ensure uniform vector scaling, while voice signals undergo spectral subtraction and Voice Activity Detection (VAD) to isolate meaningful segments, preparing both modalities for accurate and secure encrypted feature extraction.

4.2.5 Mathematical Security Guarantees:

Paillier's encryption ensures semantic security through encryption randomness, while its additive homomorphic property enables secure aggregation without decryption. Biometric, voice, and NLP-derived data remain protected throughout, as expressed by:

$$E(x_1 + x_2) = E(x_1) * E(x_2) \ (\mathrm{mod}\, n^2) \tag{4}$$

This methodology yields a resilient and secure execution pipeline capable of performing fully encrypted authentication, task authorization, and command execution in a cloud environment. No biometric, voice, or NLP-derived data is ever decrypted during operation.

4. Results and Evaluation

We evaluated the system on a dataset consisting of 10,000 facial images (adapted from publicly available face datasets [7]) and over 500 hours of voice data from LibriSpeech [11]. Our test environment used Paillier encryption implemented with PySEAL and cloud deployment through AWS EC2 and Lambda.

4.1 *Biometric Matching Performance:*

The system achieved a facial recognition accuracy of 96.2% in the encrypted domain and a voice command classification accuracy of 94.6%. Latency measurements indicated efficient performance, with an average of 1.08 seconds per frame for facial recognition, 0.9 seconds for voice parsing, and a total of 2.8 seconds for complete cloud execution.

4.2 *Cloud Task Execution:*

Cloud task execution times were measured for key operations, with EC2 instance creation taking approximately 45 seconds, volume creation and attachment requiring 18 and 25 seconds respectively, and IAM user provisioning completing in under 40 seconds.

4.3 *Cryptographic Overhead*

The cryptographic overhead was minimal, with token generation taking 1.3 milliseconds, encryption of facial vectors averaging 5.8 milliseconds, and homomorphic distance computation completing in under 10 milliseconds.

4.4 *Security Analysis*

The system demonstrated strong security resilience, with no data leakage observed under chosen-ciphertext attack simulations. All generated tokens were verified using semantic security constraints, and role-based access logs were versioned and securely stored in AWS S3 for auditability and traceability**.**

5. Conclusion and Future Work

This paper presents a end to end secure system for cloud resource management that combines facial biometrics, voice interfaces, and homomorphic encryption. This paper replaces traditional old authentication with encrypted biometric processes and secure voice commands. This system ensures data privacy without affecting usability or performance.

Future work will also be explored by moving to independent homomorphic encryption (HE) schemes like TFHE to support full arithmetic operations with integrating blockchain-based token auditing for enhanced forensic verification also adopting federated learning techniques to personalize biometric templates without centralizing sensitive data. Furthermore, the framework can be extended for domain-specific applications, particularly in areas like agriculture and surveillance. where privacy and secure automation is highly important.

References

[1] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, in STOC '09. New York, NY, USA: Association for Computing Machinery (2009), pp. 169–178. doi: 10.1145/1536414.1536440.

[2] J. R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez, "Fully private noninteractive face verification," *IEEE Transac-*

tions on Information Forensics and Security, vol. 8, no. 7, pp. 1101–1114 (2013), doi: 10.1109/TIFS.2013.2262273.

[3] M. K. Morampudi, M. V. N. K. Prasad, M. Verma, and U. S. N. Raju, "Secure and verifiable iris authentication system using fully homomorphic encryption," *Computers and Electrical Engineering*, vol. 89 (Jan. 2021), doi: 10.1016/j.compeleceng.2020.106924.

[4] G. E. Hinton, L. Deng, D. Yu, G. E. Dahl, A. R. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. N. Sainath, and B. Kingsbury, "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups," *IEEE Signal Process Mag*, vol. 29, no. 6, pp. 82–97 (2012), doi: 10.1109/MSP.2012.2205597.

[5] A. Nautsch, A. Jimenez, I. Gomez, J. Freire, J. Galbally, and J. Fierrez, "Privacy-Preserving Speaker Recognition with Cohort Score Normalisation,"(Jul. 2019), [Online]. Available: http://arxiv.org/abs/1907.03454

[6] S. Halder and T. Newe, "Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT," *Future Generation Computer Systems*, vol. 133, pp. 351–363 (Aug. 2022), doi: 10.1016/j.future.2022.03.032.

[7] P. Kumar, L. Raja, P. K. Soni, and K. Gaur, "Mathematical morphology based lung segmentation using multiscale dense pyramid network architecture," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 4, pp. 1139–1149 (Jun. 2024), doi: 10.47974/JDMSC-1969.

[8] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Springer-Verlag (1999).

[9] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "TFHE: Fast Fully Homomorphic Encryption Over the Torus," *Journal of Cryptology*, vol. 33, no. 1, pp. 34–91 (Jan. 2020), doi: 10.1007/s00145-019-09319-x.

[10] T. Ahonen, A. Hadid, and M. Pietikä, "Face Description with Local Binary Patterns: Application to Face Recognition." [Online]. Available: http://www.ee.oulu.fi/research/imag/texture/lbp/bibliography/

[11] M. P. Morolong, F. B. Shava, and A. M. Gamundani, "Cloud computing security in health cyber physical systems," Journal of Discrete Mathematical Sciences and Cryptography, vol. 26, no. 5, pp. 1553–1568 (2023). DOI: 10.47974/JDMSC-1821

[12] S. Rampal, M. Sharma, and P. Khurana, "Crypt analysis of multi-key biometric encryption for business enterprises using cloud storage," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1559–1568 (2025). DOI: 10.47974/JDMSC-2154

Received May, 2025