Enhancing Privacy in E-Payment Systems Using Homomorphic Encryption for Secure Authentication

Samuel Habtamu
HiLCoE, School of Computer Science and Technology, Addis Ababa, Ethiopia
samuelhabtamu511@gmail.com

Animaw Kerie
HiLCoE, School of Computer Science and Technology, Addis Ababa, Ethiopia
animkmu@gmail.com

Abstract

With the global rise of electronic payment (e-payment) systems, the demand for secure and privacy-preserving authentication mechanisms has become increasingly critical. Traditional methods often expose sensitive user data during verification, leading to privacy risks. This study addresses the limitations of conventional authentication techniques by proposing a homomorphic encryption (HE)-based solution that ensures data confidentiality throughout the authentication process.

The core objective of this research is to develop and evaluate a prototype authentication system that integrates iris biometrics and encrypted contextual verification specifically involving transaction timestamp, merchant identity, and payment amount while ensuring all computations occur on encrypted data. The system leverages the TenSEAL library to implement the CKKS scheme for approximate homomorphic encryption, enabling vectorized operations on encrypted biometric features and metadata without decryption. Authentication decisions are based on cosine similarity of encrypted iris features and homomorphic comparison of encrypted contextual parameters against expected values.

Methodologically, the system is tested using the IITD Iris Database v1.0, with preprocessing via PCA and normalization to reduce dimensionality and improve efficiency. Privacy was assessed using Reconstruction Attack Analysis, Ciphertext Expansion Analysis, Ciphertext Distribution Analysis, and Chosen Ciphertext Attack Simulation. Results demonstrate that the system is effectively preserved privacy, while maintaining acceptable matching accuracy and operational feasibility in a controlled environment.

Despite these achievements, the system's performance under real-world conditions remains to be validated. Limitations include its reliance on a controlled iris dataset, a limited scope of contextual parameters, and the computational overhead of HE. This research contributes a unique integration of fully homomorphic encryption into biometric authentication for e-payment systems and demonstrates its potential to provide strong

privacy guarantees without compromising security or usability.

Keywords: - Privacy, E-Payment, Homomorphic Encryption, Security, Authentication

1. Introduction

With the rapid growth of e-commerce and online transactions globally, electronic payment systems (EPS) have become a critical enabler for businesses and consumers alike. EPS provides convenient, efficient, and secure methods for transferring funds electronically over computer networks [1]. Another study noted that concern for security and privacy is the most important factor influencing the adoption of e-banking [2].

While e-payment systems offer numerous advantages, they also present significant privacy challenges. A critical point of vulnerability is the authentication process, where users provide sensitive personal data such as usernames, passwords, biometric information, and payment credentials. Conventional authentication methods such as passwords, PINs, and unencrypted biometric matching require data decryption for verification, which exposes them to potential breaches and unauthorized access. This vulnerability becomes particularly severe in cloud-based and third-party systems where data is often outsourced for processing.

Homomorphic Encryption (HE), which enables computation on encrypted data, presents a promising solution. It ensures that sensitive data never needs to be decrypted during authentication. Recent advancements, such as the CKKS scheme for approximate arithmetic, allow for secure yet practical implementations of privacy-preserving authentication systems.

Despite their growing use, biometric authentication methods in e-payment systems pose critical challenges to privacy. Biometric traits like iris patterns are immutable if compromised, they cannot be reissued. Current solutions often require partial or full decryption for verification, undermining user privacy.

Existing HE-based systems have focused mostly on either biometric template protection or secure transmission of transaction metadata. Few have integrated both into a unified, privacy-preserving system. Additionally, previous works have inadequately addressed practical attack scenarios such as reconstruction or ciphertext inference, treating privacy as a theoretical benefit rather than a measurable performance criterion.

This research aims to explore the application of Homomorphic Encryption in e-payment authentication by addressing the following key questions:

1. How can Homomorphic Encryption be effectively applied in e-payment authentication?
2. What are the privacy and performance trade-offs when using Homomorphic Encryption?
3. How resilient is HE-based authentication to real-world data breaches and attacks?

Homomorphic encryption is a form of encryption that allows specific types of computations to be carried out on ciphertexts and generate an encrypted result that, when decrypted, matches the result of operations performed on the plaintexts. This is a desirable feature in modern communication system architectures [3].

In traditional encryption methods, data must be decrypted before processing, creating a vulnerability window where the data can be exposed. Homomorphic encryption addresses this by ensuring that computations such as verifying login credentials, checking transaction histories, or performing user-specific risk assessments are conducted entirely on encrypted data. Thus, the user's sensitive information remains protected throughout the authentication process. Moreover, homomorphic encryption can allow Encrypted password matching, Secure biometric authentication & multi-factor authentication

Modern e-payment systems have redefined the way and the speed with which financial transactions can be achieved, as well as the convenience it offers across a number of digital platforms. It has also brought concerns regarding privacy, security, and authentication. Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. On the other hand, security is the combination of people, policies, processes, and technologies employed to protect sensitive data. In the domain of e-payments, this will protect against breaches and fraud from happenings like financial or biometric data. Meanwhile, Authentication is a process that verifies the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. Robust mechanisms of authentication therefore involve validation of transaction-related parameters such as legitimacy of the vendor, accuracy of transaction amount and intent of the user in authorizing the specific payment.

By integrating homomorphic encryption into e-payment systems, privacy concerns related to authentication can be significantly mitigated. It allows users to retain control over their data, reduces trust dependencies on intermediaries, and provides a higher level of security while maintaining the efficiency and usability of modern e-payment solutions. As homomorphic encryption technology continues to advance, it holds great potential to reshape privacy protection in the digital payment landscape.

2. Related Work

With the growth of e-payment facilities, ease and challenges in data privacy and security have increased. With the rapid increase in digital transactions, it is becoming essential to protect sensitive details such as authentication credentials and personal data to minimize risks like a data breach, fraud, and unauthorized access.

In early work, [4] proposed a privacy-preserving authentication system using HE where the adversary could potentially control both the client and server. This threat model emphasized encrypted verification of credentials (e.g., passwords or biometrics), ensuring

no raw data exposure during authentication. Various studies have looked at the application of homomorphic encryption (HE) in biometric template protection and in fact, some of them have gone ahead to prove the designs [5] [6]. Even so, homomorphic encryption is quite a recent technology that still has a lot of challenges that need to be solved for it to be used for biometric template protection by everyone [7]. Despite these challenges, more research is being done in this field [8]'s research sheds light on a novel method ensuring security to the biometric two-factor authentications with the incorporation of Functional Encryption (FE) into the Universal Composability (UC) framework. Particularly, this framework is based on function hiding inner product functional encryption fh-ipfe. This allows the encrypted biometric templates for instance Hamming distance, Euclidean distance, or Cosine similarity to be computed with the distances processed but no biometric information is provided. This aids in private authentication in which decisions can be made without disclosure of sensitive information [4]. While [4] emphasize fh-IPFE, other scholars have investigated other HE methods for confidential bio-authentication. There are some other HE techniques that are used for privacy-preserving biometric authentication systems. For example, [9] proposed a new packing scheme in somewhat homomorphic encryption (she) to improve the efficiency of operations on ciphertexts. This could be useful for further developments in optimizing biometric authentication performance [9].

A biometric trait that is utilized for eligibility checks is iris recognition. Iris recognition is known for its accuracy because Iris patterns are unique and stable which makes it increasingly more common in security applications [10]. There have been attempts by researchers to combine Iris recognition with HE. In this context, a very efficient implementation of HE in iris recognition is the computation of the Hamming distance of encrypted iris templates. The Hamming distance is a metric that represents the difference between two iris codes that is their binary images encoded with the iris's unique traits; the smaller the distance obtained the better the match [4]. In this way, servers do not have to access any raw data yet can still determine whether the live iris being presented corresponds to the one already enrolled.

Several studies have investigated the effectiveness of HE in preserving privacy in the context of iris authentication. For instance, [11] surveyed the existing applications of homomorphic encryption and talked about the implemented improvements in confidentiality over the years. Research conducted by [10] is based on fully homomorphic encryption (FHE) applies to iris recognition and addresses the problem of template protection while maintaining high performance and low complexity by using a batching technique [10]. In this line, the authors also propose an improvement to recognition accuracy by utilizing rotation-invariant iris codes to mitigate the problem of rotation inconsistencies. Other researchers, including [12] and [13], have explored FHE's application to various aspects of iris authentication, such as ciphertext authentication and security analysis [12] [13].

[10] provides evidence that the use of HE in iris recognition comes with challenges. For example, because HE comes with a level of privacy protection, quantum attacks have been shown to partially compromise them. In some cases, auxiliary data (AD) is needed for some implementations, which may potentially compromise security. On the contrary, Fully Homomorphic Encryption (FHE) provides biometric security that supports practical use as it allows polynomials to operate on encrypted data thus expanding its theoretical scope of usage [14]. Furthermore, the improvement of FHE technology has changed the negative outlook on its performance in the real world, and the application of FHE has become realistic [15].

A review by [5] discusses various HE-based solutions for biometric template protection, revealing that while HE offers superior privacy guarantees, its computational demands remain a barrier to widespread adoption. The study also acknowledges the need for efficient encryption schemes tailored to biometric data types. Advanced schemes like the Fan-Vercauteren (FV) and CKKS models have also been tested in iris and fingerprint recognition, enabling secure operations such as cosine similarity computation on encrypted vectors. While these models show theoretical robustness, studies like [7] and [12] caution that practical deployment remains hindered by ciphertext expansion and latency. In another direction, research by [16] employed elliptic curve cryptography (ECC) in e-payment authentication. Though not homomorphic, ECC provides lightweight encryption suited for mobile platforms and shows a trend toward optimizing performance alongside security.

Recent advances in biometric template protection have increasingly leveraged homomorphic encryption to address privacy concerns while maintaining authentication accuracy. [17] pioneered the integration of blockchain technology with additive ElGamal homomorphic encryption for multi-instance iris authentication, achieving 0.13% EER on CASIA-V3-Interval while eliminating reliance on honest-but-curious server assumptions. [18] combined EfficientNet-B7 with CKKS fully homomorphic encryption and Bloom filters for iris recognition, achieving 99.98% accuracy with 756.95ms verification time through multi-ciphertext encryption strategies. [19] introduced adaptive multi-biometric fusion (AMB-FHE) using the BFV scheme, demonstrating that sequential cascaded decision-level fusion reduced secondary biometric presentations by 72-96% while achieving 0.08% EER on combined iris and fingerprint datasets. [20] presented the first retina-based authentication with fully homomorphic encryption, achieving 0.101% EER on the RIDB database with 156ms computation time using the BFV scheme at 192-bit security level. These studies collectively demonstrate that homomorphic encryption schemes whether partial (ElGamal, Paillier), somewhat (CKKS), or fully homomorphic (BFV) effectively preserve biometric template privacy without compromising authentication accuracy, though computational overhead remains significant, with optimization strategies including feature compression, multi- ciphertext encoding, SIMD operations, and adaptive fusion proving essential for practical deployment.

Furthermore, studies on fingerprint and facial recognition systems like [21], [22], and [23] demonstrate that integrating HE with high-dimensional biometric data requires additional preprocessing (e.g., PCA or deep learning feature extraction) to manage computational load. Despite using secure encryption schemes, these systems often compromise usability or scalability.

3. The Proposed Solution

To address the challenge of ensuring privacy during e-payment authentication, this study proposes a novel privacy-preserving framework that integrates iris biometric authentication with contextual transaction verification, both performed entirely on encrypted data using Homomorphic Encryption (HE). The core aim is to prevent the exposure of sensitive user data—such as biometric identifiers and transaction metadata—during authentication, thereby mitigating the risk of data breaches, surveillance, and identity theft.

3.1 System Design and Architecture

The proposed system is structured into two core authentication phases, both executed under encryption:

1. Biometric Verification Phase
   - Utilizes iris images as the biometric identifier.
   - Images undergo preprocessing and Principal Component Analysis (PCA) to extract and reduce the dimensionality of feature vectors.
   - The CKKS scheme of the TenSEAL library is used to encrypt these vectors.
   - To determine the match between the query and stored iris templates, cosine similarity was computed. A similarity threshold of 0.7 was experimentally selected based on iterative testing with different threshold values. This threshold provided the best trade- off between maintaining privacy and minimizing the false positive rate, ensuring that authentication remains both secure and accurate.

Table 1- Results for different thresholds

Threshold	True Negative	True Positive	False Negative	False Positive
0.8	249,757	912	208	3
0.75	249,750	963	157	10
0.725	249,746	971	149	14
0.7	249,744	973	147	19
0.675	249,730	987	129	34

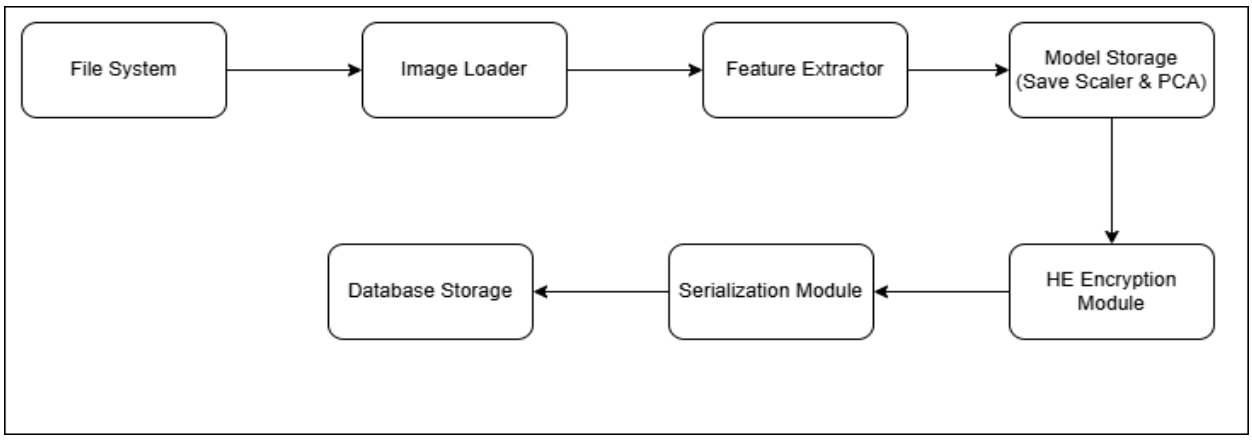

Figure 1 - Encryption and Storage

2. Contextual Verification Phase
    - Includes additional transaction-specific metadata: timestamp, merchant identity, and transaction amount.
    - This metadata is encoded and encrypted, also under the CKKS scheme.
    - The system performs homomorphic comparison operations between the encrypted values and the expected transaction context to verify integrity and authenticity.

3. Decision Logic

    A transaction is approved only if the following conditions are satisfied:

    - Biometric Match: At least one iris feature vector meets or exceeds the similarity threshold.
    - Context Match: All encrypted transaction parameters fall within acceptable bounds.
    - If either condition fails, the transaction is rejected

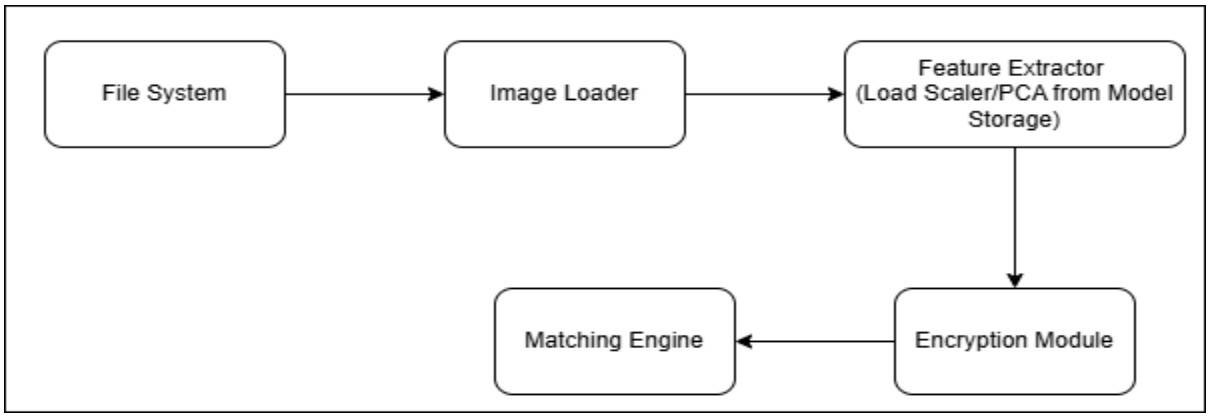

Figure 2 - Authentication Protocol I

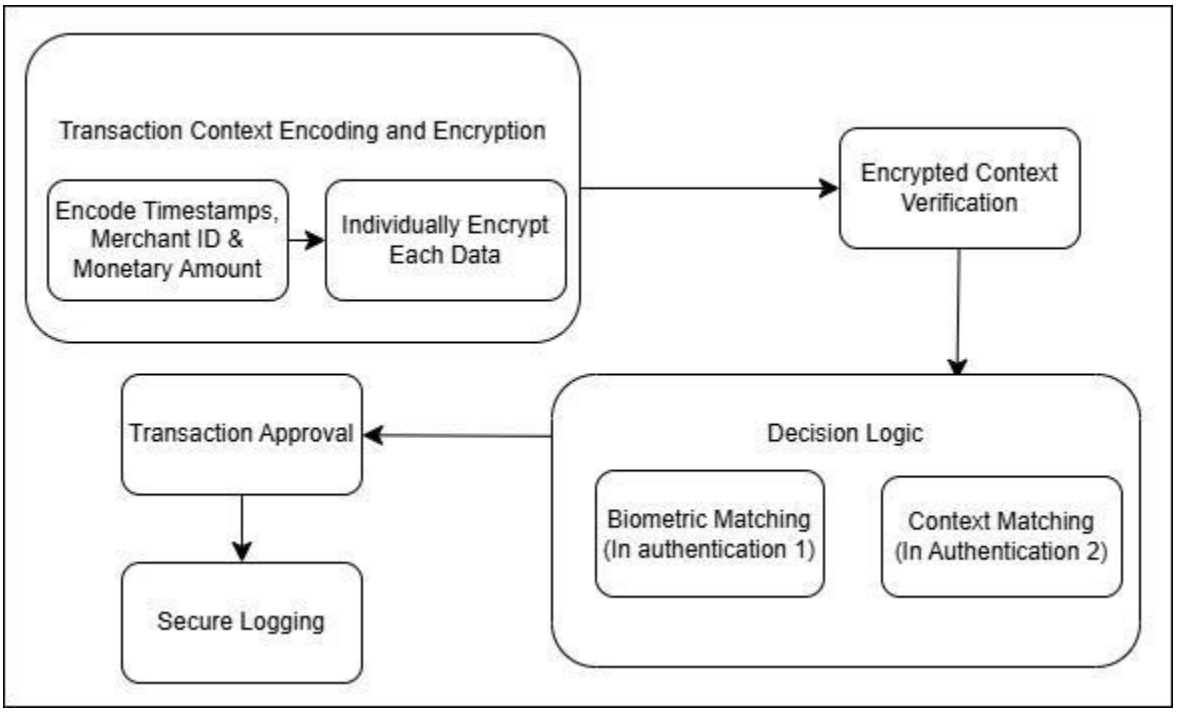

Figure 3 - Authentication Protocol II

Final authentication is granted only if both encrypted biometric and encrypted contextual verifications succeed, enabling a robust two-factor privacy-preserving authentication system.

4. Discussion

The proposed homomorphic encryption-based authentication system was evaluated based on two primary dimensions: authentication accuracy and privacy protection. The system was tested using the IIT Delhi Iris Database (v1.0) [24], employing homomorphic computations via the CKKS scheme as implemented in the TenSEAL library.

4.1. Accuracy Evaluation

Dataset and Experimental Setup

- Dataset: 1120 iris samples from 224 subjects, each matched against 224 reference entries.
- Total comparisons: 1120 × 224 = 250,880 match attempts.
- Threshold: Cosine similarity ≥ 0.7 was used for classification.

Classification Outcomes

- True Positive (TP) = 970
- False Positive (FP) = 19

- False Negative (FN) = 147
- True Negative (TN) = 249,744

Computed Metrics

- Accuracy = (TP + TN) / Total = 99.93%
- Precision (PPV) = TP / (TP + FP) = 98.18%
- Recall (TPR) = TP / (TP + FN) = 86.87%
- F1 Score = 2 × (P × R) / (P + R) = 92.13%
- FPR = FP / (FP + TN) = 0.0076%
- FNR = FN / (FN + TP) = 13.16%
- Specificity (TNR) = TN / (TN + FP) = 99.99%

4.2 Privacy Evaluation

The privacy robustness of the system was tested against multiple attack scenarios, including ciphertext analysis and decryption attempts.

Reconstruction Attack Analysis

- Reconstruction Error: 0.0000, indicating that only legitimate decryption yields the original biometric features and any unauthorized reconstruction results in unusable data.

Ciphertext Expansion

- Original Vector Size: ~400 bytes
- Encrypted Size: ~295,000 bytes
- Expansion Ratio: 740.04× on average, ranging from 737.22× to 741.57×.

Ciphertext Distribution Analysis

- Mean Byte Value: 125.12 (expected: 127.5)
- Variance: 5629.06 (expected: ~5461)
- Shannon Entropy (H_s): 7.97 bits (maximum = 8.0)
- Normalized Entropy (H_n): 0.9960

These results show that the ciphertext is statistically close to random, offering strong resistance to frequency and inference attacks.

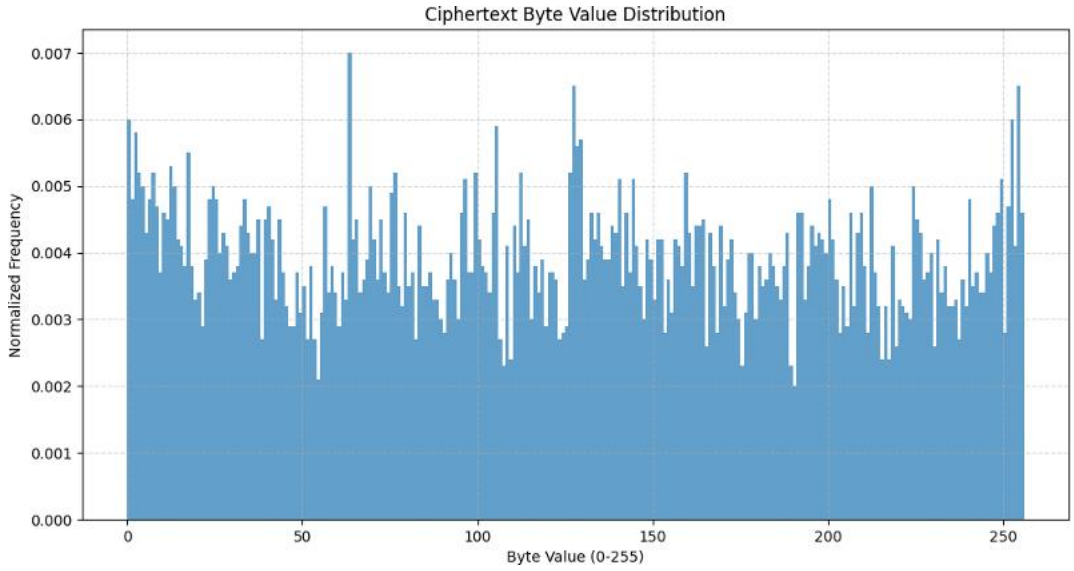

Figure 3 - Ciphertext Byte Value Distribution

Chosen Ciphertext Attack (CCA) Simulation

- Mean of Reconstructed Features: -5.02×10^{23}
- Variance: 3.95×10^{52}
- Range: -1.03×10^{27} to 1.14×10^{27}
- Average Cosine Similarity ($\bar{S}$): 0.0003

These values confirm that decrypted outputs under CCA simulation resemble random noise and are not meaningfully correlated with the original features.

Table 2 - Proposed authentication system Vs Existing system.

Aspect	**Proposed System**	**E-Ticketing System (PHE-based Card Authentication)** [25]	**Sensor-Based Authentication** [26]
Privacy	High (zero reconstruction error, CCA	Moderate (PHE limits attack surface)	Moderate (sensor data obfuscation)

	resistance)		
Accuracy	High (99.93% accuracy, strong F1-score)	Not specified, likely moderate	High (continuous monitoring)
Computational Overhead	High (CKKS encryption/decryption, 740× ciphertext expansion)	Moderate (PHE simpler than CKKS)	Low (optimized for resource efficiency)
Storage Requirements	Very high (740× expansion ratio)	Moderate (token-based storage)	Low (sensor data lightweight)

5. Conclusion and Future Work

The research work shows the advantages of the CKKS-based homomorphic encryption for protecting iris biometrics data while securing high authentication accuracy. The privacy metrics evaluation inferred that the decryption operation performed by the legitimate parties yields exact matches to the original iris feature vectors evidenced through a reconstruction error test thereby confirming that the actual biometric information can be revealed only through authorized operations. Nearly maximum Shannon entropy and uniform distribution were shown in the ciphertext analysis, which considerably mitigates the threat of statistical and inference attacks.

The evaluation further validates the robustness of the authentication system through its resistance to CCA. Statistical analyses of reconstructed feature vectors revealed deviations of extreme measures, where the mean is -5.02×10^{23}, and variance amounts to 3.95×10^{52}. These further confirm that no structured patterns exist. The minimum and maximum values from -1.03×10^{27} to

1.14×10^{27} indicate that the attack was unable to produce anything meaningful interpretations of the source biometric data. Moreover, the average pairwise cosine similarity of 0.0003 indicates that the reconstructed features remain essentially uncorrelated and distinguishable as a random noise. Hence, this shows the privacy effectiveness of the system under such attacks, that even when decrypted, the extracted data will be unusable. Together with almost Shannon maximum entropy and a uniform distribution of ciphertext, it also proves effective in counteracting statistical and inference attacks. Therefore, it strengthens its credibility in real-world authentication scenarios.

To summarize, the suggested system promises better privacy and security, demonstrated by zero reconstruction error and robust resistance to chosen ciphertext attacks. Such approaches, however, require enormous space and computational overheads with CKKS, while partial homomorphic encryption is more efficient but lacks privacy flexibility and is worse against sophisticated attacks. Biometric authentication delivers greater accuracy but would require specific infrastructures to capture and secure any particular store, making it

less adaptable for some applications. Having said that, since our system shows a ciphertext increase of 740×, it is unsuitable for resource-constrained environments, such as mobile payments, which favor lighter alternatives like sensor- based or token-based ones. It thus excels in privacy preservation but faces challenges in terms of real-time deployment and scalability, putting the spotlight on the need for further optimization or the development of hybrid solutions to compromise security, efficiency, and practicality.

The Recommended future works are:

- Optimize computational overhead of CKKS encryption: Explore integration of CKKS with conventional symmetric encryption to reduce processing time while maintaining security.
- Extend attack scenario analysis - Evaluate the system against additional privacy threats beyond chosen ciphertext attacks.
- Investigate ciphertext compression methods - Develop or apply compression techniques to reduce ciphertext storage requirements while preserving encryption integrity.
- Improve feature dimensionality reduction - Use advanced feature extraction methods to lower biometric vector size without compromising matching accuracy.

References

[1] S. Abrazhevich, Electronic payment systems: a user-centered perspective and interaction design, TUE Research Portal, 2004. [Online]. Available: https://research.tue.nl/files/2396269/200411085.pdf. [Accessed: 25-Sep-2024].

[2] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989.

[3] X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption and Applications, Springer International Publishing, 2014.

[4] J. Ernst and A. Mitrokotsa, "A Framework for UC Secure Privacy-Preserving Biometric Authentication using Efficient Functional Encryption," Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2023/481.pdf. [Accessed: 27-Sep-2024].

[5] G. Crihan, L. Dumitriu, and M. V. Crăciun, "Preliminary Experiments of a Real-World Authentication Mechanism Based on Facial Recognition and Fully Homomorphic Encryption," Appl. Sci., vol. 14, no. 2, 2024. [Online]. Available: https://www.mdpi.com/2076- 3417/14/2/718/pdf.

[6] J. Kim et al., "Secure fully homomorphic authenticated encryption," IEEE Access, 2021. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/9312710/09500126.pdf.

[7] A. Pradel et al., "Privacy-Preserving Biometric Matching Using Homomorphic Encryption," arXiv preprint, 2021. [Online]. Available: https://arxiv.org/pdf/2111.12372.

[8] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Leveled Fully Homomorphic

Signatures from Standard Lattices," Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2014/897.pdf. [Accessed: 29-Oct-2024].

[9] F. Yasuda, Y. Kogure, and K. Hanaoka, "Secure pattern matching using somewhat homomorphic encryption," in Proc. 2013 ACM Workshop Cloud Comput. Security Workshop, 2013, pp. 65– 76.

[10] M. V. Prasad, U. S. N. Raju, and M. Kumar, "Privacy-preserving iris authentication using fully homomorphic encryption," Multimedia Tools Appl., vol. 79, no. 27, pp. 19215–19237, 2020.

[11] J. Yang et al., "A review of homomorphic encryption for privacy-preserving biometrics," Sensors, vol. 23, no. 7, p. 3566, 2023.

[12] X. Song, Z. Chen, and D. Sun, "Iris ciphertext authentication system based on fully homomorphic encryption," J. Inf. Process. Syst., vol. 16, no. 3, pp. 599–611, 2020.

[13] A. Torres, N. Bhattacharjee, and B. Srinivasan, "Privacy-preserving biometrics authentication systems using fully homomorphic encryption," Int. J. Pervasive Comput. Commun., vol. 11, no. 2, pp. 151–168, 2015.

[14] J. Fan and F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption," Cryptology ePrint Archive, 2012. [Online]. Available: https://eprint.iacr.org/2012/144.pdf.

[15] M. Barni et al., "A privacy-compliant fingerprint recognition system based on homomorphic encryption and finger code templates," in Proc. 4th IEEE Int. Conf. Biometrics: Theory, Appl., Syst. (BTAS), 2010, pp. 1–7.

[16] M. Chaudhry et al., "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography," Electronic Commerce Research, vol. 16, pp. 113–139, 2016.

[17] Mahesh Kumar, Morampudi, Munaga VNK Prasad, and U. S. N. Raju. "BMIAE: blockchain-based multi-instance iris authentication using additive ElGamal homomorphic encryption." *IET Biometrics* 9, no. 4 (2020): 165-177.

[18] Fouda, E. M., Elsaid, S. A., Abdelhay, E. H., & Mohamed, M. A. A. (2025). Advanced Iris Recognition Framework using EfficientNet And Fully Homomorphic Encryption with Bloom Filters. *International Journal of Telecommunications*, *5*(02), 1-22.

[19] Bayer, Florian, and Christian Rathgeb. "AMB-FHE: Adaptive Multi-biometric Fusion with Fully Homomorphic Encryption." arXiv preprint arXiv:2503.23949 (2025)

[20] Palma, D., & Montessoro, P. L. (2024). For Your Eyes Only: A Privacy-Preserving Authentication Framework Based on Homomorphic Encryption and Retina Biometrics. *IEEE Access*.

[21] H. Choi et al., "Blind-Touch: Homomorphic Encryption-Based Distributed Neural Network Inference for Privacy-Preserving Fingerprint Authentication," Proc. AAAI Conf. Artif. Intell., vol. 38, no. 20, pp. 21976–21985, 2024.

[22] S. Ma et al., "A secure face-verification scheme based on homomorphic encryption and

deep neural networks," IEEE Access, vol. 5, pp. 16532–16538, 2017.

[23] Q. Wei et al., "Achieve efficient and privacy-preserving online fingerprint authentication over encrypted outsourced data," in Proc. IEEE Int. Conf. Commun. (ICC), 2017, pp. 1–6.

[24] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal identification," in Proc. CVPR 2008, Anchorage, AK, Jun. 2008.

[25] F. Kerschbaum, H. W. Lim, and I. Gudymenko, "Privacy-preserving billing for e-ticketing systems in public transportation," in Proc. 12th ACM Workshop Privacy Electron. Soc., 2013, pp. 143– 154.

[26] L. Hernández-Álvarez, J. M. de Fuentes, L. González-Manzano, and L. Hernández Encinas, "Privacy-preserving sensor-based continuous authentication and user profiling: a review," Sensors, vol. 21, no. 1, p. 92, 2020.