Journal of Information Systems Engineering and Management
2025, 10(12s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Secure Cancelable Fingerprint Authentication for Cloud Services

Narender. M [1], Dr. S. Thaiyalnayaki [2]
[1]*Research Scholar, Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India*
[2]*Associate Professor, CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India*
Corresponding Author Email: narikits@gmail.com

ARTICLE INFO

Received: 18 Nov 2024

Revised: 30 Dec 2024

Accepted: 18 Jan 2025

ABSTRACT

Traditional password-based authentication systems create difficulties for users while remaining vulnerable to security breaches. The solution under consideration establishes biometric-based cloud service access, which enables users to terminate their services whenever needed. The minutia cylinder code is a great local descriptor for fingerprint authentication in public databases. It meets security needs and protects privacy, while still using the advantages of biometric technology. The cancelable fingerprint template design has two key parts: a simple way to create cancelable features and a method for making adjustable, partial cancelable features. The first part employs encoding-nested-difference (XOR), while the second part contains a basic reindexing procedure. The implementation of the proposed template design has led to reduced public database storage requirements and time needs on FVC2002 DB1–DB3 and FVC2004 DB1–DB3, with a 0.21% false acceptance rate and a 0.2% improved EER, and TPR/TNR stood at 99% throughout testing. The system delivers improved security because both stolen biometric templates become useless along with the addition of new biometric samples during re-enrolment. The system implements multi-factor authentication by combining cancelable biometrics with multiple factors. The performance study demonstrates exceptional accuracy combined with minimum false acceptance and rejection rates, which makes it a good means for secure cloud access.

Keywords: Biometrics, cancelable templates, fingerprint authentication, privacy-preserving

1. Introduction

Security controls need implementation rapidly because cloud services expanded swiftly to protect vital information properly along with maintaining user privacy requirements. Authentication backups based on traditional methods like passwords and PINs remain exposed to multiple cyber threats, which make them susceptible to theft or loss. A promising authenticating solution is based on biometric authentication that utilizes unique behavioural together with physiological traits. Biometric systems with classic methodologies face difficulties since they allow template theft attacks and make modifications to the data irreversible. Cancelable biometrics presents itself as an effective solution for these problems. The conversion of biometric data into immutable formats boosts both privacy and security aspects of cloud service biometric authentication systems [1]. A transformation function changes the biometric data before storing it in the system. This process is known as cancelable biometrics. Due to its repeatability, it can apply this change again during verification. If the modified biometric data is compromised, we can "cancel" the old template by generating a new one using a different transformation function [2]. The method ensures the original biometric data's protection and undetectability, even in the event of a compromised cancelable template. There are many advantages to incorporating cancelable biometrics into cloud services. It solves, first and foremost, the problem of irreversibility that has plagued conventional biometric systems for a long time [3]. Cancelable biometrics, which enables the regeneration of biometric templates, allow users to change their credentials, similar to changing a password, in the event of biometric data hacking.

Such attacks are prevented through non-invertible cancelable templates because they cannot allow the reconstruction of authentic biometric data from modified templates [4]. Cancelable biometric systems help users achieve greater data privacy protection. Traditional biometrics create privacy challenges because of both the identity-linkage of user information and its permanent characteristic of unalterable biometric data. The use of cancelable templates prevents

the storage of biometric data, which reveals user biometric traits. The preservation of privacy-protecting functions becomes essential within cloud environments because major data breaches have widespread effects in these scenarios. Experts have introduced multiple methods for developing cancelable biometric templates, which demonstrate varying degrees of security complexities. Bio hashing provides a hashing solution that produces a unique value by combining an individual key with their biometric data for cancellation template use. Randomly changing the order of biometric traits creates new ways to authenticate, as mentioned in sources [5, 6]. Applying these techniques practically renders the restoration of the original biometric data impossible, even with knowledge of the transformation function. Cancelable biometrics in cloud services receive support from existing data security regulations and business standards. A system to protect personal data through biometrics operates based on GDPR requirements. Cloud service providers can meet GDPR data protection requirements by using cancelable biometric systems. This helps them avoid financial and legal issues. Several advantages exist when implementing cancelable biometrics in cloud services, although they present specific challenges. Achieving appropriate safety levels challenges the user-friendly factor when deciding on technological solutions. False rejection rates tend to increase when recognition accuracy suffers due to secure transformation mechanisms [8, 9]. To create an optimal system, users must have both secure access and an easy-to-use interface. When implementing cancelable biometrics in current cloud platforms, organizations need to analyze both compatibility and system integration requirements [10]. Cancelable biometrics is a new development that greatly improves the security and privacy of cloud-based biometric authentication systems.

Cancelable biometrics allows us to change biometric data into a form that can be destroyed and cannot be returned to its original state. This helps solve two main issues with regular biometric systems: the risk of data leaks and the problem of permanent changes to the data. This research focuses on developing easy-to-manage fingerprint templates that will protect identity data in authentication systems that use cloud services. The system uses the robust local descriptor minutia cylinder code (MCC), which provides high authentication capabilities on public fingerprint databases. The central purpose is to protect cloud-based biometric data privacy through an in-depth description of system development.

2. Related works

In recent years, the possibility of cancelable biometrics to improve privacy and security in cloud services has become a hot topic. This section provides a comprehensive overview of the current state of cancelable biometric systems by reviewing relevant research and technical developments, focusing on important approaches, applications, and issues in the field.

In [11], the authors developed a novel biometric authentication system to provide authorized access to a distant server in the cloud. They used a user's biometric data like a secret credential, creating a different identity from it before using it to build a private key. Another thing they came up with was a method to efficiently create a session key for secure message transmission between two parties using two biometric templates. This eliminates the need to save the user's private key anywhere and creates the session key without revealing any prior information. The system employs various security checks, including an official one based on the Real-Or-Random (ROR) model, which is capable of withstanding a variety of active and passive attacks. Finally, a comparison analysis and comprehensive testing demonstrate the efficacy and practicality of the suggested method.

In [12], the authors presented a framework for the proper adoption and adjustment of machine learning (ML) methods used to design biometric authentication systems based on electrocardiograms (ECGs). Scientists and programmers working on biometric identification systems that use electrocardiograms (ECGs) might benefit from the suggested framework by using it to better specify the scope of necessary datasets and acquire high-quality training data. They used use-case analysis to determine the extent of dataset collection. The implementation of ECG-based authentication resulted in the development of three distinct use cases for authentication purposes. Increasing the quantity and quality of training data suitable for machine learning algorithms will boost the accuracy level of biometric authentication based on ECG through machine learning methods. Using an ECG time-slicing method that focuses on the R-peak helps the system gather good training data for machine learning. The suggested architecture incorporates four additional metrics for measuring the quality of the data used for ML training and testing. They also build and make it publicly available as a Matlab toolbox, incorporating all the suggested processes, measurements, and sample data, along with examples of various ML approaches. Researchers can use this framework to organize

machine learning settings, create training data, and develop three examples for using ML in ECG biometric authentication. Researchers using machine learning (ML) can use this framework to create high-quality datasets for training and testing, use new measurement methods, and create new strategies in different areas of study.

In [13], the authors included preventing unauthorized access to systems intended to protect user privacy and strengthening security in IoTs through fingerprint authentication. Capturing fingerprints might compromise the security and privacy of personal information. They suggested Biometric Authentication Frameworks (BAFs) as a solution to privacy and security issues in Internet of Things (IoT) settings. These BAFs would enable IoT authentication in conjunction with fingerprint authentication on consumer devices at the edge, as well as guarantee biometric security in transmissions and databases. They proposed a hybrid system that combines Hybrid Advanced Encryption Standards and Chaotic Map Encryptions, as well as the Honeywell Advanced Encryption Security-Cryptography Measure (HAES-CM). BAFs allow IoT and edge devices in Industry 4.0 to communicate privately and securely. In terms of processing speed, the proposed HAES-CM encryption strategy in this study performs better than previous encryption approaches.

In [14], the authors outlined a straightforward authentication method for Internet of Things (IoT) devices to use with cloud servers. They found out that their method could be tracked and had security problems, like the risk of someone pretending to be another user, leaking verification information, and being vulnerable to insiders with special access. To fix these issues, they suggested a lightweight authentication technique that is both secure and provably secure. The suggested method protects critical parameters by encrypting the user data and secure key. It keeps computing costs low while providing rapid and real-time services to users in IoT by only using exclusive OR and hash functions. They used an RoR model and informal security analysis, which can withstand several attacks.

In [15], the authors created completely distorted templates from the ground up. The main contribution is a new security system that uses evolutionary algorithms and RNA/DNA sequences to create unique random characteristics for biometric security. The suggested system creates disorganized biometric templates by encrypting the important features that differentiate biometrics for authorized users. Get the first users started by making several encrypted biometric images using the logistic map. The next step was to decrypt it and transform them into vectors for a binary array. They then transform them into the appropriate introns and exons, updating the cloud database with the correct codons. After generating encrypted RNA lists, they substituted these relevant codons with new ones. They use extensive pixel permutations to retrieve the encryption key for each template from the initial biometric picture. Using the GA optimization method, they select the best biometric characteristics. Finally, they use the chosen traits in GA-based mutation and crossover procedures to create cancelable biometric traits. They evaluated the suggested architecture by taking into account six distinct biometric databases. All the evaluation measures used show that the suggested framework performs better in the simulations. The histograms exhibit greater uniformity, the correlation for authentic users is strong, and all biometric characteristics remain hidden.

Finally, a potential way to improve privacy and security is to include cancelable biometrics in cloud services. This article reviews several methodologies and approaches that show how cancelable biometrics may solve some problems with standard biometric systems. This might lead to better authentication systems in the cloud.

3. Materials and Methods

The proposed system contains an enrolment and verification process (see Figure 1). The enrolment process creates and stores a user's template to register them, while the verification process generates a query user's template to compare it with the enrolled user. Typically, the enrollment process involves obtaining fingerprints using a fingerprint sensor, followed by the generation and storage of templates. Typically, the verification process includes collecting fingerprints, generating a template, and then comparing the two. Applications running on the cloud first send end-user fingerprints there to generate, store, and match templates. The end user is responsible for taking a fingerprint, uploading it to the cloud, and receiving the verification result. The fact that the cloud stores personally identifiable information (such as fingerprints) raises security concerns.

Minutia extraction

All identification algorithms for fingerprints strongly rely on important features called minutiae because they serve as the main extraction targets during this critical process. The unique features used for match verification consist of

minutiae points, including ridge endings and bifurcations. The fingerprint image acquisition device using the embedded fingerprint sensor produces m minutiae elements which form $T = \{T_1, T_2, ..., T_m\}$.

Generation of Cancelable Template

The character vector T contains a static length without any safeguard mechanisms installed. An attack on vector T containing original fingerprint minutia features would generate serious privacy and security threats because it would constitute a violation of privacy rights. To safeguard vector T, we construct a cancelable fingerprint template. $V = [d, a]$ is the representation of an MCC feature, where d is the "cell value vector" and a is the "cell validity vector".

Length-Flexible Partial-Cancelable Features

This method ensures that biometric templates can manage input data of varying lengths, utilize only a subset of available characteristics, and allow for cancellation to protect user privacy. The proposed method generates a partial-cancelable feature by re-indexing the original MCC feature, which includes two parts: the cell value and whether the cell is valid. The time duration of the new cancelable feature is defined by specifying a percentage (p). The index set J of the MCC feature vector gets defined through the length L_d.

$$J = \{1,2, \ldots . K_d\} \quad (1)$$

$$d = (d_1, d_2, \ldots, d_{K_d}) \quad (2)$$

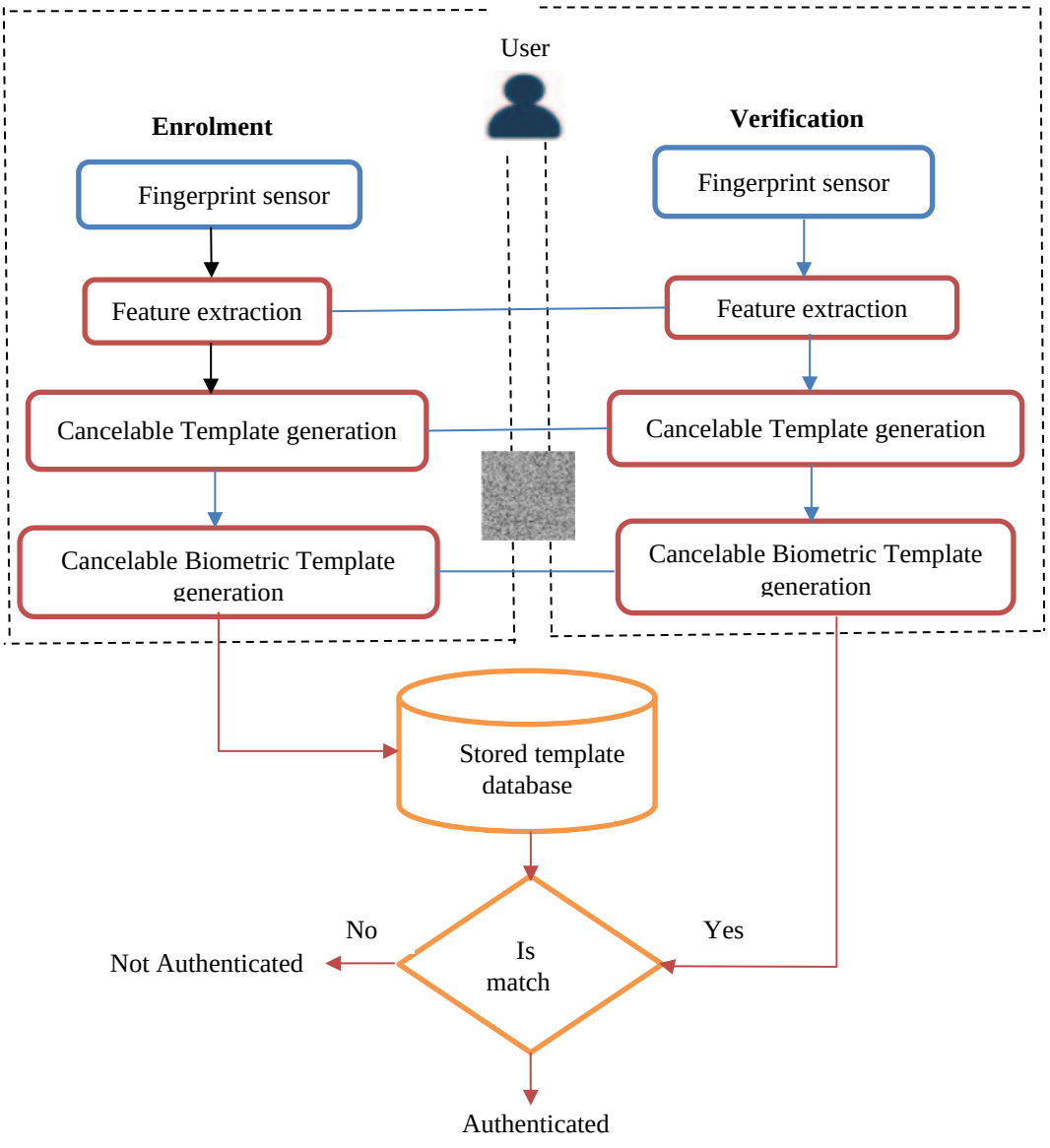

Fig. 1. Bock diagram of fingerprint authentication system.

Facilitating the acquisition process of the cell validity part happens through the duplication of the “base mask” of the cylinder. The base mask runs throughout all sections, which eliminates confusion between sections.

$$a = \left(a_1, a_2, \dots, a_{K_d}\right) \quad (3)$$

Each bit a_j within the *j*th position reveals the validity status of the *j*th cell data value in the part called *d*. The selection process for forming reindexing set *J′* involves choosing *k* different integers randomly from set *J*.

$$J' = \left\{s_j | s_j \in J, 1 \le j \le k\right\} \quad (4)$$

$$d' = \left(d_{s1}, d_{s2}, \dots, d_{s_{8h}}\right) \quad (5)$$

$$a' = \left(a_{s1}, a_{s2}, \dots, a_{s_{8h}}\right) \quad (6)$$

In general, the “partial-cancelable feature” is written as

$$V' = [d', a'] \quad (7)$$

Lightweight Cancelable Features

A secure method in biometric security changes fingerprint data, face images, and iris patterns into protected information. This allows users to easily cancel and then restore their data if there is a system breach. A partial cancelable feature with p = 50% contains 8K cell values that become 2H bits through the proposed lightweight feature application. The core operation involves computing the nested difference between the values of four nearby cells to determine the main value. We obtain the first layer nested difference vector element $c^{K_1}$from definition (8) using data from vector *d* in its original form (5).

$$c_j^{K_1} = d_{s_{2j-1}} - d_{s_{2j}} \quad (8)$$

where 1 ≤ i ≤ 4k. The “second-layer nested difference vector” c^{K_2} is then considered upon the “first-layer nested difference”, signified by

$$c^{K_2} = \left(c_1^{K_2}, c_2^{K_2}, \dots, c_{2h}^{K_2}\right) \quad (9)$$

where the *j*th element

$$c_j^{K_2} = c_{2j-1}^{K_1} - c_{2j}^{K_1}$$

$$= (d_{s_{4j-3}} - d_{s_{4j-2}})(d_{s_{4j-1}} - d_{s_{4j}})$$

The formula (16) determines the element known as t_{qp} in the scoring matrix *t*. Next, Algorithm 1 applies the "local greedy similarity (LGS)“ algorithm to the score matrix *t* to determine the decision score. A higher decision score indicates a greater matching probability between the query and registered templates; the score may be anything from 0 to 1.

Local Greedy Similarity (LGS): We employ the Local Greedy Similarity (LGS) method for pattern matching in biometric identification, such as fingerprint matching. The algorithm's primary goal is to greedily maximize the degree of similarity between two collections of characteristics, such as fingerprint minutiae points.The input sample features are denoted as $S = \{s_1, s_3, \dots . s_m\}$, whereas the template features are denoted as $T = \{t_1, t_3, \dots . t_n\}$. If we provide additional properties, such as the type of minutia, we can represent each feature s_i and t_j by their location (e.g., coordinates (x, y)) and orientation. To measure how similar two features are, one may use a similarity function, denoted as sim(s_i, t_j). One or more of the following may serve as the basis: orientation difference, Euclidean distance, or both.

Algorithm 1: Local Greedy Similarity

1. Set an initial matching score M=0.

2. Initialize an empty set P to store matched pairs of features.

3. For each feature $s_i \in S$:

4. Find the feature $t_j \in T$ that maximizes the similarity function:

5. $t_j = arg \max_{t \in T} sim(s_i.t)$

6. If $sim(s_i.t_j)$ is above a predefined threshold τ

7. Add the pair $(s_i.t_j)$ to the set P.

8. Update the matching score:

9. $M = M + sim(s_i.t_j)$

10. Optionally, remove tj from T to prevent it from being matched again.

The algorithm continues until all features in S have been processed or no more pairs can be matched above the threshold τ.

The final matching score M.

The set of matched pairs P.

4. Results and Discussion

The experiment was conducted using the Anaconda Python platform on an Intel Core i5-equipped system with 8 GB of RAM. The proposed authentication method was thoroughly tested using two public fingerprint databases, including FVC2002 DB1-DB3 and FVC2004 DB1-DB3. The FVC2002 database functions as an essential resource for research in the field of biometrics testing and fingerprint recognition system evaluation. Each dataset contains 880 images of 110 fingerprints with a total collection of four databases named DB1, DB2, DB3, and DB4. The images are captured using various sensors and artificial acquisition methods to reflect the unpredictable nature of real-world situations. The data files we present for distribution exist in BMP format with different image resolution levels. The database includes all types of fingerprint features, with a collection of high-quality images that have problems due to pressure, wrong rotation, and misalignment. The capacitive sensor inside DB3 operates alongside optical sensors that run DB1 and DB2.

A controlled assessment of DB4 involves the employment of the SFinGe fingerprint generation software program. FVC2002 offers extensive database content, making it an essential research instrument for the development, testing, and optimization of fingerprint recognition algorithms. FVC2004 offers four databases consisting of 800 digital images of 100 fingerprints with eight impressions per finger. The fingerprint data collection for these databases combines different sensor-based data alongside manufactured fingerprints to ensure a wide range of features and quality. The fingerprint images in FVC2004 present varied resolutions because the sensors used in practical applications operate at different levels. The evaluation process of fingerprint verification strength requires datasets containing different resolution images ranging from high detail to low detail. Using true positive rate (TPR) along with accuracy, equal error rate (EER), false rejection rate (FRR), false acceptance rate (FAR), and true negative rate (TNR) showed that the suggested method works well in real-life situations. The FVC 2002 and FVC 2004 databases provided a variety of fingerprint data types for testing the proposed technique. We evaluated the proposed method by taking into account FAR, FRR, TPR, TNR, and EER. Table 1 presents the parameters applied to the FVC2002 dataset information. The FVC2004 dataset received the same parameter evaluation as shown in Table 2.

Table 1. Performance assessment of cancelable method on the FVC2002 dataset.

No. of FP Samples	FAR (%)	FRR (%)	TPR (%)	TNR (%)	EER (%)
100	0.15	0.11	98.98	98.53	1.32
200	0.18	0.13	98.65	98.78	1.54
300	0.20	0.16	99.11	98.88	1.65
400	0.15	0.15	98.86	99.11	0.2
500	0.21	0.22	99.12	99.12	1.65

The proposed cancelable method was used to analyze 500 fingerprints from the FVC2002 dataset. The TPR and TNR measurement reached a maximum level of 99.12% using the dataset provided. The proposed cancelable approaches established 0.22% as their highest FRR point by studying 500 fingerprint samples. The highest FAR remained at 0.21% for these fingerprint examples. The proposed method achieved a minimum performance level of TPR and TNR, which met 99.64% of the criteria. The proposed method reaches an EER value of 1.32% when evaluated with the FVC2002 dataset data. Figure 2 presents the values obtained from testing the FVC2002 dataset, which included FAR, FRR, and EER.

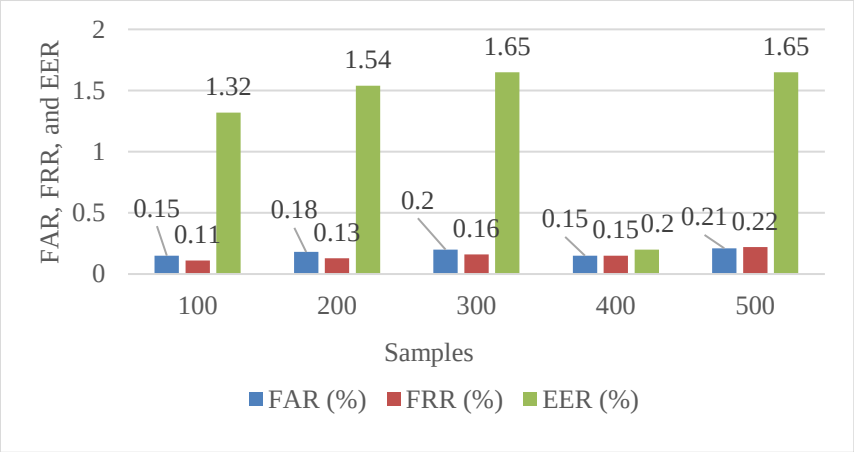

Fig.2. Plot of FAR, FRR, and EER in FVC2002 dataset.

The proposed cancelable method was tested by analyzing 500 fingerprint samples from the FVC2004 database. The dataset enabled us to achieve TPR and TNR of 99.12% as maximum values. The highest FAR reached a rate of 0.21% when using the proposed cancelable techniques to process 500 fingerprint samples along with a maximum FRR of 0.22%. Averaging the minimal values showed that TPR and TNR equaled 98.64%. The application of the proposed method against FVC2004 data reached an EER measurement of 1.41%. The FVC2004 dataset illustrates the FAR, FRR, and EER values in Figure 3.

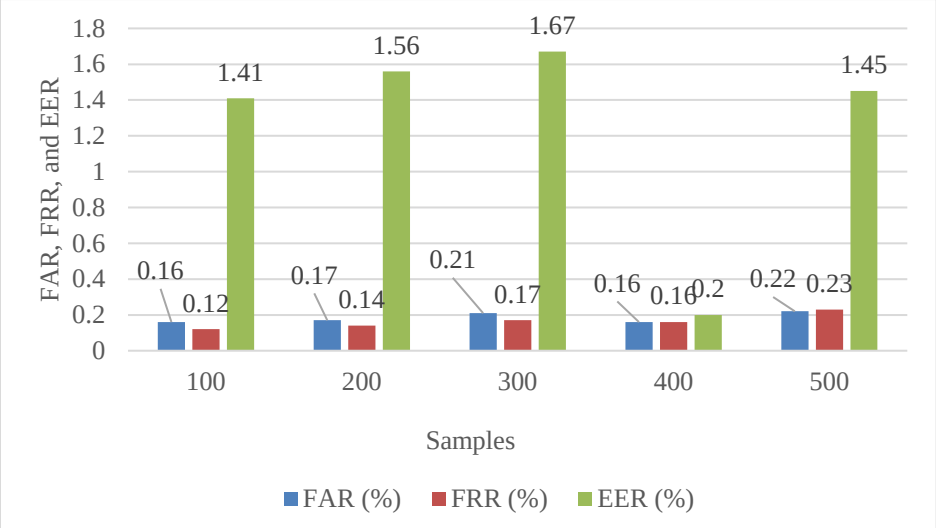

Fig.3. Plot of FAR, FRR, and EER in FVC2004 dataset.

Analysis of Computational Cost and Template Size

The following section examines both the proposed authentication method's operation resource requirements along its template measurement specifications. Table 3 presents the testing period for creating cancelable templates and original MCC-based real-valued fixed-length vector T matching.

Table 3: Average time for cancelable template generation and fingerprint matching

Avg. time	**FVC2002**			**FVC2004**		
	DB1	**DB2**	**DB3**	**DB1**	**DB2**	**DB3**
Cancelable template generation (n = 149)	4.25	4.38	4.78	4.14	4.21	4.66
Designed cancelable template	0.45	0.41	0.48	0.41	0.38	0.46
Original MCC-based feature	1.38	1.25	1.41	1.28	1.56	1.75

As shown in Figure 4, the developed cancelable template greatly reduces the average matching time compared with the baseline, which was based on the original MCC-based feature vector. The time saved in matching is because of the smaller template, since the proposed method reduces the cancelable template's length by half, with $1 < n \leq m/2$, where n is the key length.

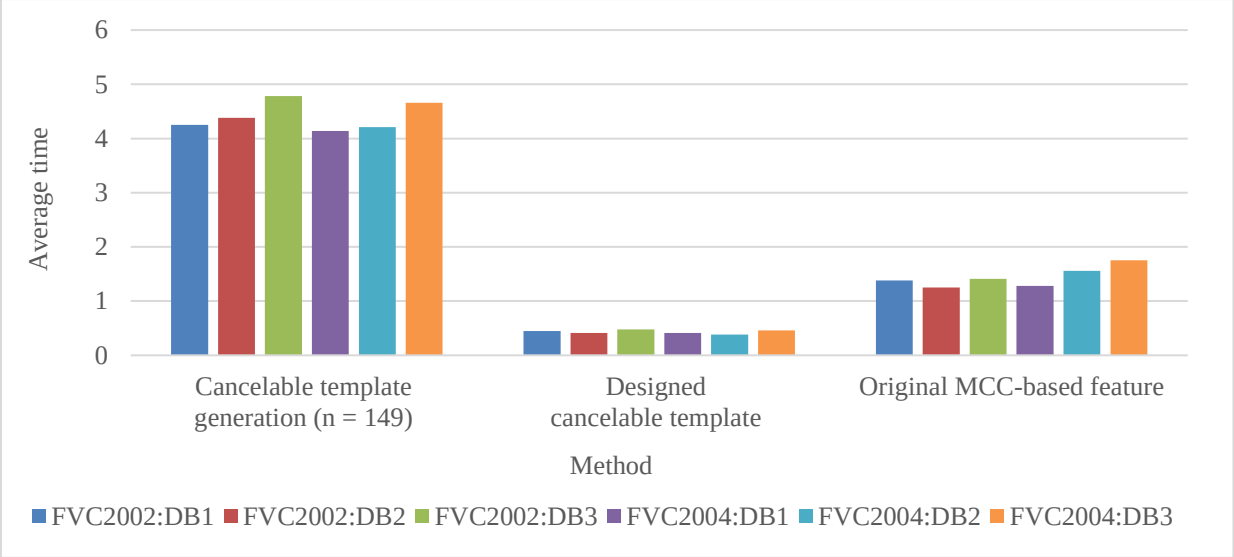

Fig.4. Performance comparsion of Computational Cost and Template Size

5. Conclusion

This paper proposes a biometric-based safe access method for cloud services, which is cancelable to prevent theft or abuse of biometric data. The system converts biometric templates, allowing for revoke and reissue of compromised data. Multi-factor authentication enhances security. The proposed template design consists of a re-indexing strategy for partial-cancelable feature creation and an encoding-nested-difference XOR technique for lightweight cancelable feature generation. The experimental results show that the proposed system maintains dependable operation by minimizing false acceptance and rejection errors while achieving strong FAR accuracy. We develop cancelable templates from FVC2002 and FVC2004 fingerprint biometric data. The proposed system achieves secure cancelable template generation on both FVC2002 and FVC2004 datasets with EER at 0.2% and FAR measuring 0.21% and 0.22% respectively. Also, it takes $1\times10^{1}5$ seconds to generate the cancelable template and $1\times10^{2}5$ seconds to match using the designed cancelable template. This makes it a viable and efficient option for strengthening cloud service security. To further improve the system's security and usability, future work will concentrate on optimizing the transformation algorithms and investigating the inclusion of other biometric modalities.

References

[1] Jin, Z., Teoh, A. B. J., & Toh, K. A. (2021). Cancelable biometrics: Concepts, methods and applications. IEEE Transactions on Information Forensics and Security, 16, 2170-2186.

[2] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. In Audio- and Video-Based Biometric Person Authentication (pp. 223-228). Springer, Berlin, Heidelberg.

[3] Soliman, Naglaa & Algarni, Abeer & El-Shafai, Walid & Abd El-Samie, Fathi & El Banby, Ghada. (2021). An Efficient GCD-Based Cancelable Biometric Algorithm for Single and Multiple Biometrics. Computers, Materials and Continua. 10.32604/cmc.2021.016980.

[4] Abd-elaziem, Ayman & Abdelhafeez, Ahmad & Soliman, Tamer. (2024). A Proposed Cancelable Biometrical Recognition System (CBRS) Based on Developed Hénon Chaotic-Map. Wireless Personal Communications. 134. 10.1007/s11277-023-10823-4.

[5] Teoh, A. B. J., Yue, S., & Ku, A. C. C. (2006). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition, 37(11), 2245-2255.

[6] Kumar, A., & Zhang, D. (2020). Improving biometric security using cancelable templates. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(2), 1044-1054.

[7] European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.

[8] Hassan, Sabit & Shaar, Shaden & Raj, Bhiksha & Razak, Saquib. (2018). Online Evaluation of Classifier Accuracy, False Acceptance Rate and False Rejection Rate.

[9] Jegede, Abayomi & Udzir, Nur & Abdullah, Azizol & Mahmod, Ramlan. (2017). Cancelable and hybrid biometric cryptosystems: current directions and open research issues. International Journal of ADVANCED AND APPLIED SCIENCES. 4. 65-77. 10.21833/ijaas.2017.011.010.

[10] Yang, Wencheng & Wang, Song & Guanglou, Zheng & Chaudhry, Junaid & Valli, Craig. (2018). ECB4CI: an enhanced cancelable biometric system for securing critical infrastructures. The Journal of Supercomputing. 74. 10.1007/s11227-018-2266-0.

[11] Banerjee, Soumya & Odelu, Vanga & Das, Ashok Kumar & Chattopadhyay, Samiran & Rodrigues, Joel & Park, Youngho. (2019). Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2926578.

[12] Kim, Song-Kyoo & Yeun, Chan & Damiani, Ernesto & Lo, Nai-Wei. (2019). A Machine Learning Framework for Biometric Authentication Using Electrocardiogram. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2927079.

[13] Altameem, Ayman & P, Prabu & Thiyagarajan, Senthilnathan & Poonia, Ramesh & Saudagar, Abdul. (2023). A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0. Systems. 11. 28. 10.3390/systems11010028.

[14] Ju, Sieun & Park, Yohan. (2023). Provably Secure Lightweight Mutual Authentication and Key Agreement Scheme for Cloud-Based IoT Environments. Sensors. 23. 9766. 10.3390/s23249766.

[15] Hossam, Fatma & El-Shafai, Walid & Elkamchouchi, Hassan & ELfahar, Adel & Alarifi, Abdulaziz & Amoon, Mohammed & Aly, Moustafa & Abd El-Samie, Fathi & Singh, Aman & Elshafee, Ahmed. (2022). A Cancelable Biometric Security Framework Based on RNA Encryption and Genetic Algorithms. IEEE Access. 10. 55933 - 55957. 10.1109/ACCESS.2022.3174350.

[16] D. Maio, D. Maltoni, R. Chappell, J. L. Wayman, and A. K. Jain, “FVC2002: Second fingerprint verification competition,” in Proc. ICPR, vol. 3, 2002, pp. 811–814

[17] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2004: Third fingerprint verification competition,” in Proc. Int. Conf. Biometric Authentication, 2004, pp. 1–7

[18] Soliman, R.F.; Ramadan, N.; Amin, M.; Ahmed, H.H.; El-Khamy, S.; Abd El-Samie, F.E. Efficient cancelable Iris recognition scheme based on modified logistic map. Proc. Natl. Acad. Sci. India Sect. A Phys. Sci. 2020, 90, 101–107.

[19] Drozdowski, P.; Garg, S.; Rathgeb, C.; Gomez-Barrcro, M.; Chang, D.; Busch, C. Privacy-preserving indexing of Iris-codes with cancelable Bloom filter-based search structures. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 2360–2364

[20] Bendib, I.; Meraoumia, A.; Haouam, M.Y.; Laimeche, L. A New Cancelable Deep Biometric Feature Using Chaotic Maps. Pattern Recognit. Image Anal. 2022, 32, 109–128.