INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

[1]PARSAM RAJANI KANTH, [2]M. SAMUEL SANDEEP REDDY

[1]PG Scholar, Dept. of MCA, Newton's Institute of Engineering, Guntur, (A.P)

[2]Associate professor, Dept. of CSE, Newton's Institute of Engineering, Guntur, (A.P)

***Abstract**:* In recent years, biometric identification has gained widespread acceptance. Database owners may be enticed by cloud computing's ability to reduce costly storage and compute expenses by moving users' massive amounts of biometric data and identification duties to the cloud, but doing so may expose users to unwanted risks. In this study, we provide a biometric identification outsourcing method that is both effective and secure. In this case, the biometric information is encrypted before being sent to a remote server in the cloud. The data query is encrypted by the database owner and sent to the cloud where a biometric identification is carried out. An identifier is applied to the encrypted database on the cloud, and the result is sent back to the database owner. Even if attackers are able to falsify identification requests and cooperate with the cloud, a detailed security study shows that the proposed technique is still safe. The experimental findings demonstrate that the suggested system outperforms the existing techniques in both the pre-processing and the identification phases.

Keywords: biometric identification; data outsourcing; privacy-preserving; cloud computing

I. INTRODUCTION

Because it offers a potential technique to identify users, biometric identification has gained a lot of attention recently.

Conventional authentication techniques, such as passwords and ID cards, are seen as less secure and more inconvenient than biometric identification [1]. In addition, biometric identification, which relies on identifying a person by one or more of their unique physical characteristics and uses data gathered from a variety of sensors [2], [3], and [4] such as a fingerprint, iris, or facial pattern, has found extensive use in many different contexts.

The FBI, which is in charge of maintaining the nation's fingerprints database, is one organisation that would want to use a cloud server (like Amazon's) to store and process the system's massive amounts of biometric data. However, biometric data encryption is necessary before outsourcing to protect privacy. FBI partners (such police departments) may request an identity verification by generating an identification query based on the subject's biometric characteristics (fingerprints, irises, speech patterns, face features, etc.).

The FBI then sends the encrypted query to the cloud in order to locate the most likely match. As a result, developing a system that permits secure and rapid biometric identification in the cloud is a significant challenge.

Several methods of biometric identification that do not compromise users' privacy have been presented [10–17]. Schemes based on homomorphic encryption and oblivious transmission for fingerprint and facial picture recognition, for example [10], [11], focus primarily on privacy protection but overlook efficiency. Once the database becomes bigger than 10 MB, these strategies become inefficient due to the limitations of local devices. In a later paper, Evans et al. [12] proposed a biometric identification approach that uses circuit design and ciphertext packing techniques to provide efficient identification for databases as big as 1GB. An effective privacy-preserving biometric identification technique was presented by Yuan and Yu [13]. In order to ensure the safety of fingerprint traits, they built three modules and developed a concrete methodology. In their plan, the database's owner sends identifying matching jobs to the cloud to boost productivity. Zhu et al. [18] noted, however, that a malevolent user and cloud may execute a collusion attack to break Yuan and Yu's protocol. To achieve biometric identification, Wang et al. [14] suggested the technique Cloud BI-II, which makes use of random diagonal matrices. However, as shown in [15], [16], their methods were insecure.

In this study, we present a biometric identity system that is both secure and easy to use, and which can withstand a collusion assault from both users and the cloud.

The following is a summary of our most significant contributions:

Our analysis of the biometric identification technique [13] reveals its flaws and the vulnerability of the system to the suggested level-3 attack. In particular, we show that an attacker may decode all users' biometric features by working with the cloud to retrieve their secret keys.

- We provide an innovative biometric authentication method that is both secure and convenient for its users. The thorough security study demonstrates that the suggested method provides enough confidentiality. Our technique can withstand the assault suggested in [18] and is safe under the biometric identification outsourcing paradigm.

- The performance study demonstrates that the proposed system offers a reduced computational cost in both the preparation and identification operations when compared to the current biometric identification techniques.

Here is how the rest of the paper is structured: The models and design objectives are presented in Section II. In Section III, we present an overview of the prior protocol suggested by Yuan and Yu, as well as a security analysis of that protocol. In Section IV, we provide a biometric identification system that is both quick and private. Section V presents the results of the security study, and Section VI assesses the results. We provide the relevant literature in Section VII and our findings in Section VIII.

II. MODELS AND DESIGN GOALS

The notations, design objectives, attack model, and system model are all introduced here.

I. MODEL OF THE SYSTEM

The database administrator, the end users, and the cloud infrastructure are all illustrated in Fig.1 as the three main players in the system.

The database administrator has access to a vast amount of biometric information (fingerprints, irises, speech patterns, facial structures, etc.) that has been encrypted before being sent to the cloud. In order to verify a user's identity, a query is made to the database administrator. The request is sent to the database owner, who then constructs a ciphertext for the biometric feature and sends it to the cloud. The cloud server deciphers the query and provides the database owner with the appropriate index. At last, the database operator delivers the user's query result after calculating the degree of similarity between the information provided in the query and the biometric information used to create the index.

Assuming the biometric data has been processed to the point where its representation may be utilised to carry out a biometric match, our technique operates on this premise. Without sacrificing generality, we take a specific aim at fingerprints, representing them using Finger Codes [19]. In particular, each digit in a Finger Code (where n = 640 and l = 8) represents a l-bit integer. If the Euclidean distance between two Finger Codes x = [x1, x2, , xn] and y = [y1, y2, , yn] is less than some threshold, then the two fingerprints are likely to belong to the same individual.

B. METHOD OF ATTACK

As stated in [13], [15], and [17], the cloud server is first and foremost a "honest but curious" entity. The cloud will always utilise the specified protocol, but it will also try to hide user and database owner information. The encrypted biometric database, encrypted queries, and encrypted matching results are all assumed to be accessible to an attacker in the cloud. The attacker may even assume the role of a user and craft completely arbitrary requests.

As a result, we divide the assault model into three categories:

Attackers at Level 1 can only read the encrypted data in the cloud. The ciphertext-only attack model [20] is followed here.

• Level 2: Similar to the known-candidate attack paradigm [21], attackers have access to the encrypted data stored in the cloud and a collection of biometric features in database D, but they do not have access to the associated ciphertexts in database C.

Attackers at this level may be legitimate users in addition to having access to all the features available at level 2. This allows attackers to fabricate as many ID queries as feasible in order to decrypt the accompanying plaintexts. This kind of attack is based on the known-plaintext attack concept [20].

If the level-(1, 2, 3) assault fails, then the biometric identification technique is safe. Keep in mind that just because the suggested approach can fend off level-2 and level-3 assaults doesn't imply an attacker may appear as a legitimate user and get access to plaintexts stored in the biometric database. Unfortunately, there is currently no fool proof way to counteract such a sophisticated assault [14].

In this research, we zero in on an attack vector whereby a malevolent user and a cloud server work together to accomplish their goals. Similar to the attack model

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

outlined in [14], the attacker is unaware of the connection between the plaintexts and ciphertexts in the biometric database.

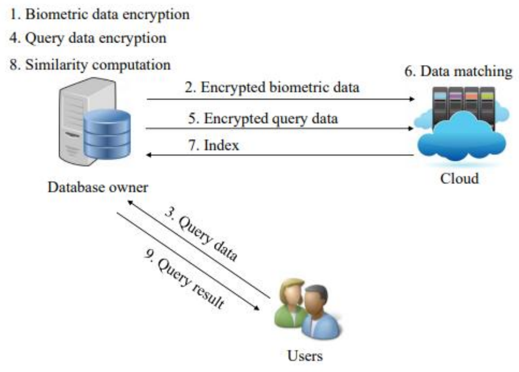


FIGURE 1. System model.

C. AIM OF THE DESIGN

The suggested strategy takes into account both security and efficiency in order to attain practicality. The following is a more detailed description of the intended outcomes of the proposed scheme's design:

The computational expenses of both the database owner and the user should be kept to a minimum for maximum efficiency. Most biometric identification processes should be run on the cloud to maximise efficiency.

Biometric information should be kept private throughout the identification procedure for reasons of security. The sensitive data must remain secret from both attackers and the dishonest cloud.

III. PERFORMANCE ANALYSIS

We deploy a cloud-based, privacy-protecting fingerprint identification system to test the efficacy of the proposed approach. We have 2 cloud nodes, each with a 6-core 2.10 GHz Intel Xelus CPU and 32GB of RAM. Our laptop has an Intel Core 2.40 GHz processor and 8GB of RAM. The database is built with random 640- entry vectors, and the query Finger Codes are chosen at random from that pool, as in [13] and [14].

Analysis of Complexity

Table 2 summarises the compute and transmission costs in our system, as well as the methods in [13] and [14], from the perspective of the data owner, the cloud server, and the users. The temporal complexity of this operation is O(m log m) for sorting fuzzy Euclidean distances, and O(n 3) for each matrix multiplication (where n is the dimension of a Finger Code). As can be seen in Table 2, the first stages of our plan involve less complications. In other words, the database owner may save money on bandwidth and calculation. Our scheme's computing complexity in the identification phase is less than that in [14]. Our method is superior because it uses vector-matrix multiplication to locate the best match, while [14] requires the use of matrix-

matrix multiplication. Our technique has the same complexity as the one described in [13], but we highlight that in order to compute Pi so quickly, [13] compromises considerable security. In addition, our method performs better since it uses less multiplication operations.

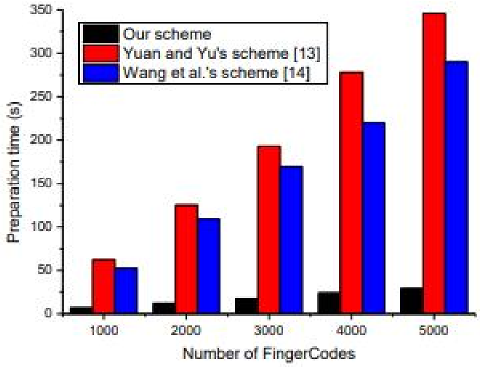


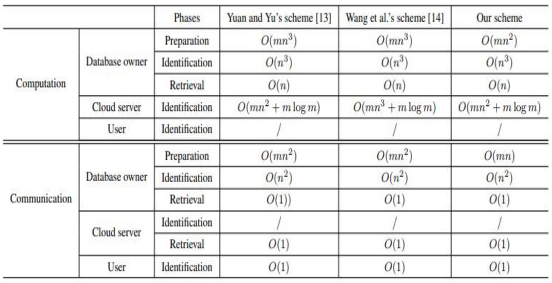
FIGURE 2. Time costs in the preparation phase.

B. EVALUATION BY EXPERIMENT

The preliminary stages. Preparation phase calculation and transmission costs for a range of 1000–5000 Finger Codes are shown in Figures 2 and 3. As can be shown in Fig.2, our technique reduces the time and effort required to register 5000 Finger Codes by 88.85 and 90.58% when compared to [13] and [14]. The reason for this is that our technique requires fewer matrix multiplication operations since just one matrix is used when encrypting a sample Finger Code. Bandwidth costs for the three strategies are shown in Fig. Our technique has a substantially lower communication cost than [13], [14] due to the fact that data is sent to the cloud in the form of vectors rather than matrices.

The spotting stages. Identification phase computation and transmission costs for a range of 1000–5000 Finger Codes are shown in Figures 4 and 5.

Figure 4 shows that when the size of the database rises, all techniques expand linearly. Our method is faster than [13] by roughly 56% due to the fact that it requires less matrix multiplication operations. By doing a vector-matrix multiplication instead of a matrix-matrix multiplication, we may reduce the time required for identification by as much as 84.75 percent in comparison to [14]. Costs in terms of bandwidth for the three systems are quite similar, as illustrated in Fig. 5. The reason for this is because during the identification phase, all schemes must send a matrix.



		Phases	Yuan and Yu's scheme [13]	Wang et al.'s scheme [14]	Our scheme
Computation	Database owner	Preparation	$O(mn^3)$	$O(mn^3)$	$O(mn^2)$
		Identification	$O(n^3)$	$O(n^3)$	$O(n^3)$
		Retrieval	$O(n)$	$O(n)$	$O(n)$
	Cloud server	Identification	$O(mn^2 + m\log m)$	$O(mn^3 + m\log m)$	$O(mn^2 + m\log m)$
	User	Identification	/	/	/
Communication	Database owner	Preparation	$O(mn^2)$	$O(mn^2)$	$O(mn)$
		Identification	$O(n^2)$	$O(n^2)$	$O(n^2)$
		Retrieval	$O(1))$	$O(1)$	$O(1)$
	Cloud server	Identification	/	/	/
		Retrieval	$O(1)$	$O(1)$	$O(1)$
	User	Identification	$O(1)$	$O(1)$	$O(1)$

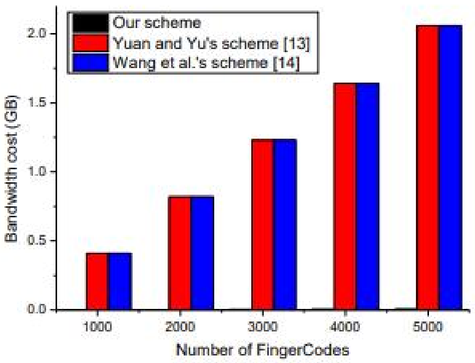


FIGURE 3. Bandwidth costs in the preparation phase.

V. CONCLUSION

In this study, we provide a unique biometric identification strategy for cloud computing that safeguards user privacy. We have developed a novel encryption algorithm and cloud authentication certification to meet the criteria for efficiency and security. The thorough examination demonstrates its resilience to any prospective threats. Furthermore, we showed the suggested approach satisfies the efficiency demand effectively via performance assessments.

REFERENCES

[1] A. Jain, L. Hong and S. Pankanti, “Biometric identification,” Communications of the ACM, vol. 43, no. 2, pp. 90-98, 2000.

[2] R. Allen, P. Sankar and S. Prabhakar, “Fingerprint identification technology,” Biometric Systems, pp. 22-61, 2005.

[3] J. de Mira, H. Neto, E. Neves, et al., “Biometric-oriented Iris Identification Based on Mathematical Morphology,” Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195, 2015.

[4] S. Romdhani, V. Blanz and T. Vetter, “Face identification by fitting a 3d morphable model using linear shape and texture error functions,” in European Conference on Computer Vision, pp. 3-19, 2002.

[5] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A survey of key management schemes in wireless sensor networks,” Journal of Computer Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.

[6] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, “An effective key management scheme for heterogeneous sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 24-34, 2007.

[7] X. Du and H. H. Chen, “Security in wireless sensor networks,” IEEE Wireless Communications Magazine, vol. 15, no. 4, pp. 60-66, 2008.

[8] X. Hei, and X. Du, “Biometric-based two-level secure access control for implantable medical devices during emergency,” in Proc. of IEEE INFOCOM 2011, pp. 346-350, 2011.

[9] X. Hei, X. Du, J. Wu, and F. Hu, “Defending resource depletion attacks on implantable medical devices,” in Proc. of IEEE GLOBECOM 2010, pp. 1-5, 2010.

[10] M. Barni, T. Bianchi, D. Catalano, et al., “Privacy-preserving finger code authentication,” in Proceedings of the 12th ACM workshop on Multimedia and security, pp. 231-240, 2010.

[11] M. Osadchy, B. Pinkas, A. Jarrous, et al., “Sci-Fi-a system for secure face identification,” in Security and Privacy (SP), 2010 IEEE Symposium on, pp. 239-254, 2010.

[12] D. Evans, Y. Huang, J. Katz, et al., “Efficient privacy-preserving biometric identification,” in Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS, 2011.

[13] Prasadu Peddi (2021), “Deeper Image Segmentation using Lloyd’s Algorithm”, ZKGINTERNATIONAL, vol 5, issue 2, pp: 1-7.

[14] Q. Wang, S. Hu, K. Ren, et al., “Cloud: Practical privacy-preserving outsourcing of biometric identification in the cloud,” in European Symposium on Research in Computer Security, pp. 186-205, 2015.

[15] Uday Chandrakant Patkar, Sushas Haribabu Patil and Prasad Peddi, "Translation of English to Ahirani Language", *International Research Journal of Engineering and Technology(IRJET)*, vol. 07, no. 06, June 2020.