International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 2nd Jan 2021. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-12

DOI: 10.48047/IJIEMR/V09/I12/155

Title: **AN EFFICIENT AND PRIVACY-PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING**

Volume 09, Issue 12, Pages: 905-909

Paper Authors

M. SUVARNA LATHA, GODALA SRILEKHA, KETHAVATH MANISHA, T.KANAKAIAH

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN EFFICIENT AND PRIVACY-PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING

M. SUVARNA LATHA[1], GODALA SRILEKHA[2], KETHAVATH MANISHA[3], T.KANAKAIAH[4]

[1,2,3,] B TECH Students, Department of CSE, Princeton Institute of Engineering & Technology For Women, Hyderabad, Telangana, India.

[4] Assistant Professor, Department of CSE, Princeton Institute of Engineering & Technology For Women, Hyderabad, Telangana, India.

Abstract: Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which however brings potential threats to users' privacy. In this paper, we propose an efficient and privacy-preserving biometric identification outsourcing scheme. Specifically, the biometric data is encrypted and outsourced to the cloud server. To execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over the encrypted database and returns the result to the database owner. A thorough security analysis indicates the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with previous protocols, experimental results show the proposed scheme achieves a better performance in both preparation and identification procedures.

Index Terms: biometric identification; data outsourcing; privacy-preserving; cloud computing

I. INTRODUCTION

Biometric identification has raised increasingly attention since it provides a promising way to identify users. Compared with traditional authentication methods based on passwords and identification cards, biometric identification is considered to be more reliable and convenient [1]. Additionally, biometric identification has been widely applied in many fields by using biometric traits such as fingerprint [2], iris [3], and facial patterns [4], which can be collected from various sensors [5]–[9]. In a biometric identification system, the database owner such as the FBI who is responsible to manage the national fingerprints database, may desire to outsource the enormous biometric data to the cloud server (e.g., Amazon) to get rid of the expensive storage and computation costs. However, to preserve the privacy of biometric data, the biometric data has to be encrypted before outsourcing. Whenever a FBI's partner (e.g., the police station) wants to authenticate an individual's identity, he turns to the FBI and generates an identification query by using the individual's biometric traits (e.g., fingerprints, irises, voice patterns, facial patterns etc.). Then, the FBI encrypts the query and submits it to the cloud to find the close match. Thus, the challenging problem is how to design a protocol which enables efficient and privacy preserving biometric identification in the cloud computing. A number of privacy-preserving biometric identification solutions [10]–[17] have been proposed. However, most of them mainly concentrate on privacy preservation but ignore

the efficiency, such as the schemes based on homomorphic encryption and oblivious transfer in [10], [11] for fingerprint and face image identification respectively. Suffering from performance problems of local devices, these schemes are not efficient once the size of the database is larger than 10 MB. Later, Evans et al. [12] presented a biometric identification scheme by utilizing circuit design and ciphertext packing techniques to achieve efficient identification for a larger database of up to 1GB. Additionally, Yuan and Yu [13] proposed an efficient privacy-preserving biometric identification scheme. Specifically, they constructed three modules and designed a concrete protocol to achieve the security of fingerprint trait. To improve the efficiency, in their scheme, the database owner outsources identification matching tasks to the cloud. However, Zhu et al pointed out that Yuan and Yu's protocol can be broken by a collusion attack launched by a malicious user and cloud. Wang et al. [14] proposed the scheme CloudBI-II which used random diagonal matrices to realize biometric identification. However, their work was proven insecure. In this paper, we propose an efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users and the cloud. Specifically, our main contributions can be summarized as follows: We examine the biometric identification scheme [13] and show its insufficiencies and security weakness under the proposed level-3 attack. Specifically, we demonstrate that the attacker can recover their secret keys by colluding with the cloud, and then decrypt the biometric traits of all users. We present a novel efficient and privacy-preserving biometric identification scheme. The detailed security analysis shows that the proposed scheme can achieve a required level of privacy protection. Specifically, our scheme is secure under the biometric identification outsourcing model and can also resist the attack proposed by. Compared with the existing biometric identification schemes, the performance analysis shows that the proposed scheme provides a lower computational cost in both preparation and identification procedures.

II. RELATED REVIEW

Related works on privacy-preserving biometric identification are provided in this section. Recently, some efficient biometric identification schemes have been proposed. Wang and Hatzinakos proposed a privacy-preserving face recognition scheme. Specifically, a face recognition method is designed by measuring the similarity between sorted index numbers vectors. Wong and Kim proposed a privacypreserving biometric matching protocol for iris codes verification. In their protocol, it is computationally infeasible for a malicious user to impersonate as an honest user. Barni et al. [10] presented a FingerCode identification protocol based on the Homomorphic Encryption technique. However, all distances are computed between the query and sample Fingercodes in the database, which introduces too much burden as the size of fingerprints increases. To improve the efficiency, Evans et al. [12] proposed a novel protocol which reduces the identification time. They used an improved Homomorphic encryption algorithm to compute the Euclidean distance and designed novel garbled circuits to find the minimum distance. By exploiting a backtracking protocol, the best match FingerCode can be found. However, in [12], the whole encrypted database has to be transmitted to the user from the database server. Wong et al.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

[24] proposed an identification scheme based on kNN to achieve secure search in the encrypted database. However, their scheme assumes that there is no collusion between the client side and cloud server side. Yuan and Yu [13] proposed an efficient privacy-preserving biometric identification scheme. However, Zhu et al pointed out their protocol can be broken if a malicious user colludes with the cloud server in the identification process. Based on [13], Wang et al. presented a privacy-preserving biometric identification scheme in [14] which introduced random diagonal matrices, named CloudBI-II. However, their scheme has been proven insecure in [15], [16]. Recently, Zhang et al proposed an efficient privacy-preserving biometric identification scheme by using perturbed terms.

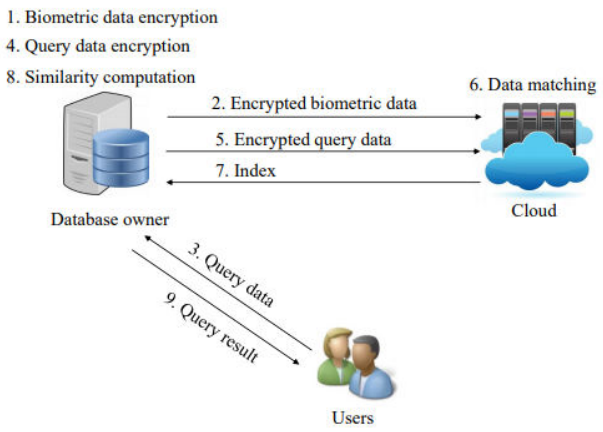

Figure 3: System model

Design Goals: In order to achieve practicality, both security and efficiency are considered in the proposed scheme. To be more specific, design goals of the proposed scheme are described as follows: **Efficiency:** Computational costs should be as low as possible at both the database owner side and the user side. To gain high efficiency, most biometric identification operations should be executed in the cloud. **Security:** During the identification process, the privacy of biometric data should be protected. Attackers and the semi-honest cloud should learn nothing about the sensitive information.

We construct a novel biometric identification scheme to address the weakness of Yuan and Yu's scheme. To achieve a higher level of privacy protection, a new retrieval way is constructed to resist the level-3 attack. Moreover, we also reconstruct the ciphertext to reduce the amount of uploaded data and improve the efficiency both in the preparation and identification procedures. In the remaining part of this section, we will introduce the preparation process and the identification process. In the preparation process, bi is the i-th sample feature vector derived from the fingerprint image using a feature extraction algorithm. To be more specific, bi is an n-dimensional vector with l bits of each element where n = 640 and l = 8. For ease of identification, bi is extended by adding an (n+ 1)-th element as Bi . Then, the database owner encrypts Bi with the secret key M1 as follows: Ci = Bi × M1. (9) The database owner further performs the following operation: Ch = M−1 2 × HT. (10) Each FingerCode Bi is associated with an index Ii. After execute the encryption operations, the database owner uploads (Ci , Ch, Ii) to the cloud.

Identification Process: The identification process includes the following steps: When a user has a query fingerprint to be identified, he/she first gets the query FingerCode bc derived from the query fingerprint image. The FingerCode bc is also an ndimensional vector. Then, the user sends bc to the database owner.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Security Analysis: In this part, we first prove that our scheme is secure under level-2 and level-3 attacks, and then we will show the proposed scheme can resist the attack proposed by Zhu et al. According to the attack scenario 2, an attacker can obtain some plaintexts of the biometric database, but does not know the corresponding ciphertexts. We consider Ci which is obtained by multiplying Bi and M1. Since the mapping relationship between Bi and Ci is not known, it is impossible for the attacker to compute Bi and M1. In the level-3 attack, besides the knowledge of encrypted data in the cloud, the attacker can forge a large number of query FingerCodes Γ as inputs. In the following, we will show the proposed scheme is secure by proving that the secret keys cannot be recovered.

Complexity Analysis: Summarizes the computation and communication costs on the data owner side, cloud server and users in our scheme and the schemes in [13] and [14]. In this work, each matrix multiplication costs O(n 3), where n denotes the dimension of a FingerCode, and the sorting cost of fuzzy Euclidean distances has time complexity of O(m log m). As illustrated in Table 2, our scheme has lower complexities in the preparation phase. That is, more computation and bandwidth costs can be saved for the database owner. In the identification phase, the computation complexity of our scheme is lower than that in [14]. The reason is that our scheme performs vector-matrix multiplication operations to find the close match, while [14] needs to execute matrixmatrix multiplication operations. Although the complexity of our scheme is the same as that in [13], we emphasize that [13] sacrifices the substantial security to achieve such fast computation of Pi . Moreover, our scheme executes fewer multiplication operations, and thus obtains better performance.

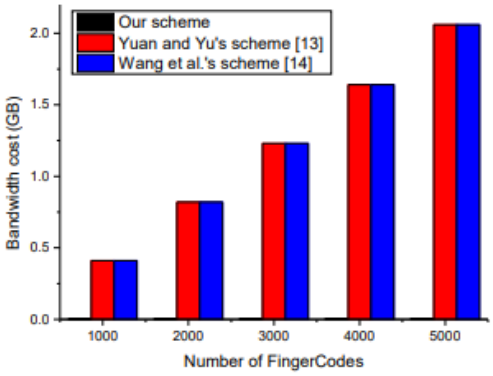

Figure 4: Bandwidth costs in the preparation phase.

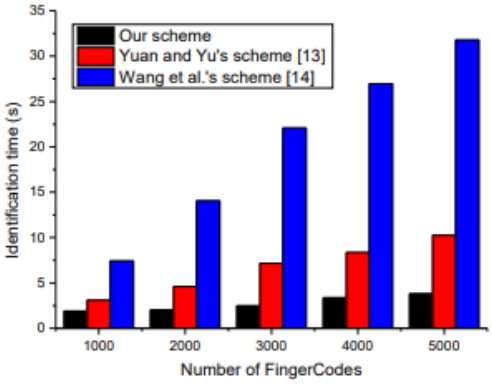

Figure 5: Time costs in the identification phase.

CONCLUSION

In this paper, we proposed a novel privacy-preserving biometric identification scheme in the cloud computing. To realize the efficiency and secure requirements, we have designed a new encryption algorithm and cloud authentication certification. The detailed analysis shows it can resist the potential attacks. Besides, through performance evaluations, we

further demonstrated the proposed scheme meets the efficiency need well.

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 fingercode 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., "SCiFI-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] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in Proc. of IEEE INFOCOM 2013, pp. 2652-2660, 2013.

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

[15] Y. Zhu, Z. Wang and J. Wang, "Collusion-resisting secure nearest neighbor query over encrypted data in cloud," In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on, pp. 1-6, 2016.

[16] S. Pan, S. Yan, and W. Zhu, "Security analysis on privacy-preserving cloud aided biometric identification schemes," in Australasian Conference on Information Security and Privacy, pp. 446-453, 2016.