International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

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

S Nandhini[1], R Sathish[2]
[1] *PG Scholar, Department of Computer Science & Engineering*
[2] *Assistant professor, Department of Information Technology*
[1&2] *KGiSL Institute of Technology, Coimbatore*

Abstract— Biometric identification has plays a vital role in achieving user authentication. For efficiency and economic savings, biometric data owners are motivated to outsource the biometric data and identification tasks to a third party, which however introduces potential threats to user's privacy. In this paper, we propose a new privacy-preserving biometric identification scheme which can release the database owner from heavy computation bur-den. In the proposed scheme, we design concrete biometric data encryption and matching algorithms, and introduce perturb terms in each biometric data. A thorough analysis indicates that our schemes are secure, and the ultimate scheme offers a high level of privacy protection. In addition, the performance evaluations via extensive simulations demonstrate our schemes' efficiency.

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

I. INTRODUCTION

Biometric identification has been widely utilized to authenticate users' identities with biometric data, which include fingerprints, irises, facial patterns, etc. Compared with the traditional authentication techniques such as passwords and identification cards, biometric identification searches the traits collections to find the best match for a given biometric trait. As biometric sensors (e.g., fingerprint sensors, etc.) are becoming smaller and cheaper, automatic identification based on biometric data is becoming an attractive alternative to the traditional authentication methods of identification.

A typical biometric identification system consists of a database owner and users. The database owner stores a set of bio-metric data and users can submit candidate biometric traits to the database owner to authenticate themselves. To release them from expensive local storage and heavy computation cost, more and more companies and governments are motivated to upload their data to the cloud for economic and storage savings. Although benefits can be obtained by utilizing the cloud, there are still some privacy issues. Thus, sensitive biometric data have to be encrypted before outsourc-ing in order to avoid the disclosure of private information. For instance, whenever a user wants to identify an individual's identity, he bank will submit the query to the database owner. Upon receiving the query, the database owner encrypts it and further turns to the cloud server for identification.

II. EXISTING SYSTEM

A number of privacy-preserving biometric identification solutions 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 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 greater than 10 MB. Later, Evans et al. presented a biometric identification scheme by utilizing circuit design and ciphertext packing techniques to achieve efficient identification for a larger database of up to1GB. Additionally propose and efficient privacy preserving biometric identification scheme. Specifically, they constructed three module sand 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 pointed out that yours protocol can be broken by a collusion attack launched by a malicious user and cloud. Proposed the scheme Cloud BI-II which used random diagonal matrices to realize biometric identification. However, their work was proven in secure in.

III. PROPOSED SYSTEM

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 and show its in sufficiencies and security weakness un-der the proposed level-3attack. Specifically, wedemonstrate that the attacker can recover their secret keys by colluding with the cloud ,and then decrypt the biometric trait so fall 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 out- sourcing 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.

IV. ARCHITECTURE DIAGRAM

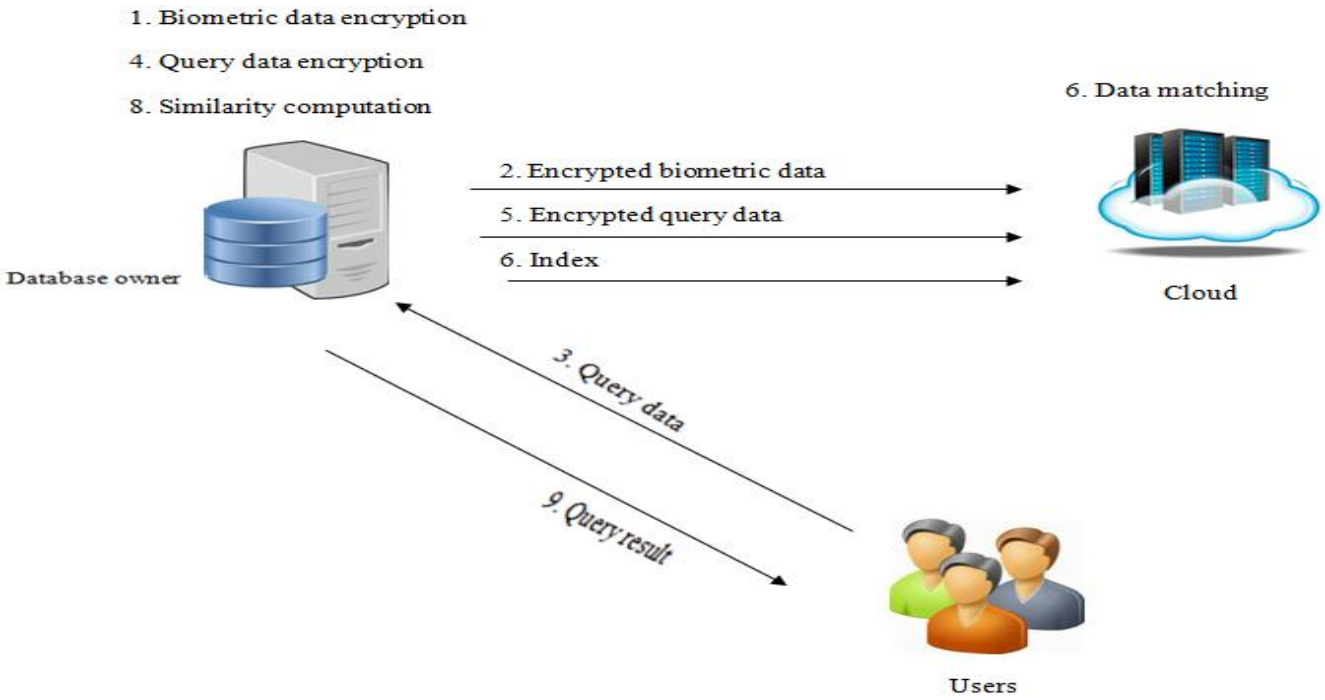

Fig.1 Overall System Architecture

V. MODULE DESCRIPTION

The proposed system is designed and implemented with the following modules such as,

- System Module
- Attacker Module

1) System Module

The database owner holds a large size of biometric data (i.e.,finger prints, irises, voice, and facial patterns etc.), which is encrypted and transmitted to the cloud for storage. When a user wants to identify himself/herself, a query request is be sent to the database owner. After receiving the request, the database owner generates a cipher text for the biometric trait and then transmits the cipher text to the cloud for identification. The cloud server figures out the best match for the encrypted query and returns there lated index to the database owner. Finally, the database owner computes the similarity between the query data and the biometric data associated with the index, and returns the query result to the user.

In our scheme, we assume that the biometric data has been processed such that its representation can be used to execute biometric match. Without loss of generality, similar to, we target fingerprints and use FingerCodes to represent the fingerprints .More specifically, a FingerCode consists of n elements and each element is a l-bit integer (typically n = 640 and l = 8). Given two FingerCodes x = [x1,x2,⋯ ,xn] and y = [y1,y2,⋯ ,yn], if their Euclidean distance is below a threshold , they are usually considered as a good match, which means the two finger print are considered from the same person.

Attack Model:

First of all, the cloud server is considered to be "honest but curious" as described in . The cloud strictly follows the designed protocol, but makes efforts to reveal privacy from both the database owner and the user. We assume that an attacker can observe all the data stored in the cloud including the encrypted biometric database, encrypted queries and matching results.

Moreover, the attacker can act as a user to construct arbitrary queries. Thus, we categorize the attack model into three levels as follows:

- Level 1: Attackers can only observe the encrypted data stored in the cloud. This follows the well-known ciphertext-only attack model.

- Level 2: In addition to the encrypted data stored in the cloud, attackers are able to get a set of biometric traits in the database D but do not know the corresponding ciphertexts in the database C , which is similar to the known-candidate attack model.

- Level 3: Besides all the abilities in level-2, attackers in level-3 can be valid users. Thus, attackers can forge as many identification queries as possible and obtain the corresponding ciphertexts. This attack follows the known-plaintext attack model.

VI. CONCLUSION

We proposed An efficient privacy-preserving biometric identification scheme in 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.