JES
Journal of Engineering Sciences
Vol 10, Issue 11, Nov /2019
ISSN NO:0377-9254

An Efficient And Privacy Preserving Biometric Identification Scheme In Cloud Computing

[1]SHAIK AYESHA, [2]M.MALLIKARJUNA REDDY, [3]A.D.SIVARAMA KUMAR

[1]M.Tech Student, [2,3]Assistant Professor
DEPT OF CSE
SVR Engineering College, Nandyal

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 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 that the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with previous protocols, experimental results show that the proposed scheme achieves a better performance in both preparation and identification procedures.

1. 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. Additionally, biometric identification has been widely applied in many fields by using biometric traits such as fingerprints, iris, and facial patterns, which can be collected from various sensors. 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 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 larger than 10 MB. Later, Evans et al. presented a biometric identification scheme by utilizing circuit design and ciphertext packing techniques to achieve efficient identification. Larger database of up to 1GB.Additionally,Yuan and Yu 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, Zhuetal.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. proposed the scheme CloudBI-II which use random diagonal matrices to realize biometric identification. However, their work was proven insecure in.

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 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. EXISTING SYSTEM:

Related works on privacy-preserving biometric identification are provided in this section. Recently, some efficient biometric identification schemes have been proposed. Wangand 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 privacy preserving 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. presented a Finger Code identification protocol based on the Homomorphic Encryption technique. However, all distances are computed between the query and sample Finger codes in the database, which

introduces too much burden as the size of fingerprints increases.

To improve the efficiency, Evans et al. 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 Finger-Code can be found. However, in the whole encrypted database has to be transmitted to the user from the database server.

Wong et al. proposed an identification scheme based on kNN to achieve secure search in the encrypted database.

2.1DISADVANTAGES:

The system doesn't implement Biometric Identification Scheme.

There is no an affective privacy preserving encryption techniques in this system.

III. PROPOSED SYSTEM

The proposed system examines the biometric identification scheme and shows 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.

The system presents 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 the proposed system.

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.**

3.1 ADVANTAGES OF PROPOSED SYSTEM:

An efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users.

Attackers can only observe the encrypted data stored in the cloud. In order to avoid, the well-known cipher text-only attack model has been implemented.

IV. SYSTEM DESIGN

4.1 System Architecture:

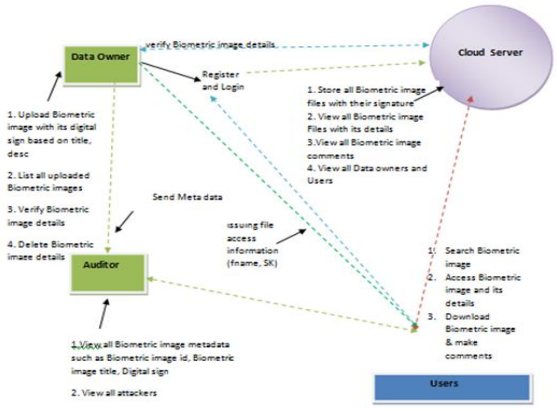

Fig : 4.1 System Architecture

V. MODULES

Data Owner:

In this module, the data owner uploads their Biometric images with their contents data to the Cloud server. For the security purpose the data owner assigns the digital sign and then store in the Cloud and also performs the following operations such as Upload Biometric image with its digital sign based on title, desc, List all uploaded Biometric images, Verify Biometric image details, and Delete Biometric image details.

Cloud Server:

The Cloud service provider manages a Cloud to provide data storage service. And performs the following operations such as Store all Biometric image files with their signature, View all Biometric image Files with its details, View all Biometric image comments, View all Data owners and Users, and View all attackers.

User:

The Cloud User who has a large amount of data to be stored in Cloud Servers and have the permissions to access and manipulate stored Biometric image and its data. The consumer will search the data and accessing the Biometric image data if he is authorized and performs the following operations such as Search Biometric image, Access Biometric image and its details, Download Biometric image & make comments.

VI. 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.

11. 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]Y.Zhu,Z.WangandJ.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.

[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] H. Delfs, H. Knebl, and H. Knebl, "Introduction to cryptography," Berlin etc.: Springer, 2002.

[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.