AN EFFICIENT AND PRIVACY PRESERVING BIOMETRICS IDENTIFICATION SCHEME IN CLOUD COMPUTING

Mohammed Shahrukh[1], Rafi Hussain[2], Shaikh Farhan[3], Abdul Rais[4]
B.Tech Students[1, 2, 3,] Assistant Professor[4]
Department of Computer Science & Engineering
Lords Institute of Engineering and Technology, Himayat Sagar, 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. With the rapid growth in the development of smart devices equipped with biometric sensors, client identification system using biometric traits are widely adopted across various applications. Among many biometric traits, fingerprint-based identification systems have been extensively studied and deployed. However, to adopt biometric identification systems in practical applications, two main obstacles in terms of efficiency and client privacy must be resolved simultaneously. That is, identification should be performed at an acceptable time, and only a client should have access to his/her biometric traits, which are not revocable if leaked. Until now, multiple studies have demonstrated successful protection of client biometric data; however, such systems lack efficiency that leads to excessive time utilization for identification. The most recently researched scheme shows efficiency improvements but reveals client biometric traits to other entities such as biometric database server. This violates client privacy. In this paper, we propose an efficient and privacy-preserving fingerprint identification scheme by using cloud systems.

Keywords: Cloud User, Cloud Owner

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. Additionally, biometric identification has been widely applied in many fields by using biometric traits such as fingerprint 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 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 all. presented a biometric identification scheme by utilizing circuit design and ciphertext packing techniques to achieve efficient identification for a volume 4, 2016 IEEE Access and Transaction on Cloud Computing, Volume:6, Issue Date:26. March.2018 larger database ofupto1GB.

II.BASIC STRUCTURE OF A BIOMETRIC SYSTEM

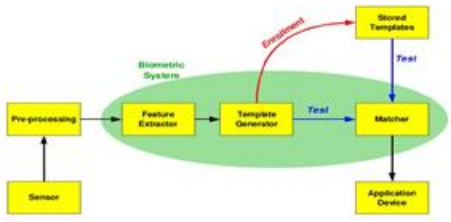


Fig 2.1 Basic Structure of a Biometric System

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login).During

Enrollment, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. Biometric recognition can be used in

Identification mode, where the biometric system identifies a person from the entire *enrolled* population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

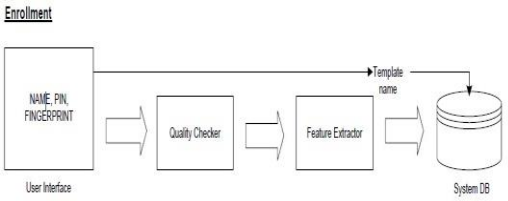


Fig.(a) Enrollment of user

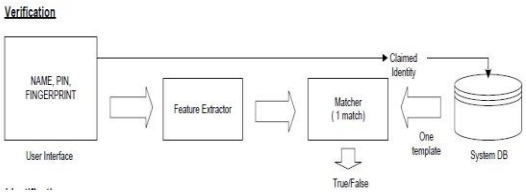


Fig.(b) Verification of user

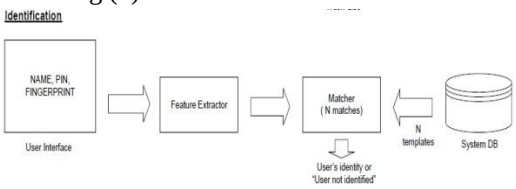
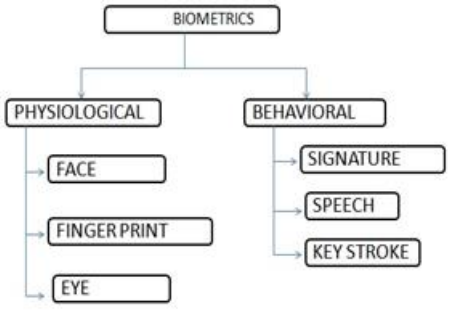


Fig.(c) Identification of user

CLASSIFICATION OF BIOMETRICS



Biometrics encompasses both physiological and behavioral characteristics. A physiological characteristic is a relatively stable physical feature such as finger print, iris pattern, retina pattern or a Facial feature. A behavioral trait in identification is a person's signature, keyboard typing pattern or a speech pattern. The degree of interpersonal variation is smaller in a physical characteristic than in a behavioral one.

III IMPLEMENTATIONS

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 attacker

Users

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

IV.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]Du,Y.Xiao,M.Guizani,andH.H.Chen,"Aneffectivekey 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,andX.Du,"Biometric-basedtwo-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 GLOBE COM 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 Symposiumon ,pp. 239-254, 2010.

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

[13] Y.Zhu,Z.Wangand 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.

[14] 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.