Journal of Engineering Sciences

AN EFFICIENT AND PRIVACY PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING

#1M.RUCHITHA, *M.Tech Student,*
#2M.NARENDHAR, *Associate Professor,*
DEPARTMENT OF CSE,
SCIENT INSTITUTE OF TECHNOLOGY,IBRAHIMPATNAM, RANGAREDDY,T.S.

Abstract:-Today many cloud users are facing the major problem of fake logging in and data theft. So it is required to authenticate the cloud user that requests access to an account for providing privacy and security. However, the techniques used for authentication so far were not capable to guarantee the same and thereby kept the data at high risk. In this paper, we propose a novel privacy-preserving biometric identification scheme which achieves efficiency by exploiting the power of cloud computing. In our proposed scheme, the biometric database is encrypted and outsourced to the cloud servers. To perform a biometric identification, the database owner generates a credential for the candidate biometric trait and submits it to the cloud. The cloud servers perform identification over the encrypted database using the credential and return the result to the owner. During the identification, cloud learns nothing about the original private biometric data. Because the identification operations are securely outsourced to the cloud, the real time computational/ communication costs at the owner side are minimal. Thorough analysis shows that our proposed scheme is secure and offers a higher level of privacy protection than related solutions such as *kNN* search in encrypted databases.

I. INTRODUCTION

Today Cloud Computing is becoming a hot trend in IT industries. Most of the enterprises are using cloud for storing and maintaining their huge data on cloud servers. But security of critical data over the cloud has become a concern for both cloud service users and providers. Traditional authentication mechanism like password, key generation, encryption mechanism has failed. Hackers are able to crack these passwords. So, the data is not secure until we have a secure mechanism to protect the data from intruders and hackers.

Biometric identification has became more popular in recent years. Biometric identification has been widely applied in many fields such as in Airport Security, Time and Attendance, Law Enforcement, Banking – Transaction Authentication, Control and Single Sign On(SSO) by using biometric traits such as fingerprint, iris and retina patterns, facial patterns, voice waves, DNA and signatures which can be collected from various sensors.

Biometrics in banking has increased a lot and is being implemented by banks throughout the entire world. As global financial entities become more digitally-based, banks are implementing biometric technology to improve customer and employee identity management in an effort to combat fraud, **increase transaction security**, and enhance customer convenience. People are getting fed-up with identity theft and the inconveniences associated with constantly having to prove their identities. As a result, more and more

customers are looking for banks that have biometric authentication to be placed in a bank. When compared with traditional authentication, biometric identification is considered to be more reliable and convenient and secure. Most common Biometric payment method till now is Fingerprint payment method which is done by using Fingerprint Scanning. Additionally, Biometric identification has raised increasingly used because it provides a promising way to identify authenticated users.

II. RELATED WORK

Biometric identification is a reliable and convenient way of identifying individuals. In practical applications, identification can be performed over many types of biometric traits such as fingerprint [12], face [13], iris [14], etc. Given a biometric database and a candidate biometric trait, the basic operation for identification is to compute the similarity between each item in the database and the candidate biometric trait, and find the best match given a pre-defined error bound. The similarity can be calculated using various algorithms based Euclidean distances, Hamming distances, etc. Despite the differences, these algorithms share the similar arithmetic operations such as addition and scalar product. W.l.o.g., in this work we emphasize on biometric identification using fingerprints.

For fingerprint identification, many existing works have been proposed by exploiting various features of the fingerprint [12], [13], [15], [16], [17]. In this work, we assume the filterbank-based approach [12] (also used by Barni et. al. [2] and Huang et. al. [4]) is used for extracting the fingerprint features. This is because the filterbank-based approach provides relatively better accuracy than others. Furthermore, in the filterbank-algorithm, the transformation from fingerprint images to the feature vector just involves lightweight operations using standard image-processing programs. Therefore, it can be efficiently supported by various types of clients including low-cost devices.

Biometric-oriented iris identification based on mathematical morphology

A new method for biometric identification of human irises was proposed in this paper. The method is based on morphological image processing for the identification of unique skeletons of iris structures, which are then used for feature extraction. In this approach, local iris features are represented by the most stable nodes, branches and end-points are extracted from the identified skeletons. Assessment of the proposed method was done using subsets of images from the University of Bath Iris Image Database (1000 images) the CASIA Iris Image Database (500 images).

Face Identification by Fitting a 3D Morphable Model Using Linear Shape and Texture Error Functions

A novel algorithm aiming at analysis and identification of faces viewed from different poses and illumination conditions. Face analysis from a single image is performed by recovering the shape and textures parameters of a 3D Morphable Model in an analysis-by-synthesis fashion. The shape parameters are computed from a shape error estimated by optical flow and the texture parameters are obtained from a texture error. The algorithm uses linear equations to recover the shape and texture parameters irrespective of pose and lighting conditions of the face image. Identification experiments are reported on more than 5000 images from the publicly available CMU-PIE database which includes faces viewed from 13 different poses and under 22 different illuminations.

III. PROPOSED METHOD

In the proposed project we have developed a banking application to incorporate the basic products purchase and payment methodologies. We have also proposed an efficient and privacy-preserving bio-metric identification outsourcing scheme. In order to overcome the computational cost and storage expenses our system is proposed. 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.

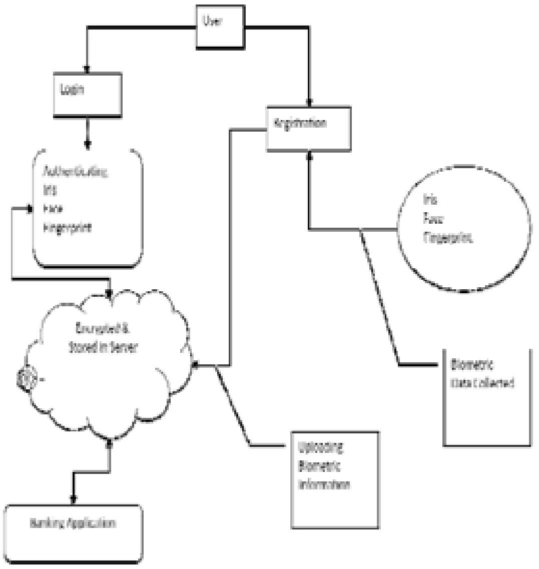


Fig.1 Architecture diagram for the proposed system

IV. ALGORITHM

In general, the BioAaaS based authentication scheme
consists of two stages:

1) Enrolment process.

2) Verification process.

The user provides biometric information i.e. fingerprint to the biometric sensor, which converts the biometric data into a binary string. The feature extractor converts the binary string into a reduced representation set of features (eliminates the redundancy). The feature vector of a user is stored into a data base of service provider. In verification process, when a user tries to log in into the remote cloud server, same steps will be executed. The feature vector is extracted by the feature extractor and submitted to matching module. The matching module intercepts the feature vector stored against user during enrolment process. The matching module executes an algorithm to check the matching similarity between enrolment and verification feature vectors for the user trying to log in. In our scheme we use standard correlation to measure the similarity matching, which is considered to be efficient for vector processing. The Figure.2.shows the architecture diagram of the system.

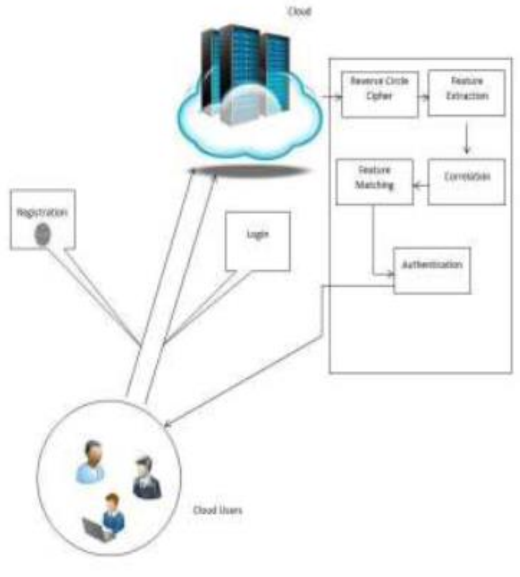
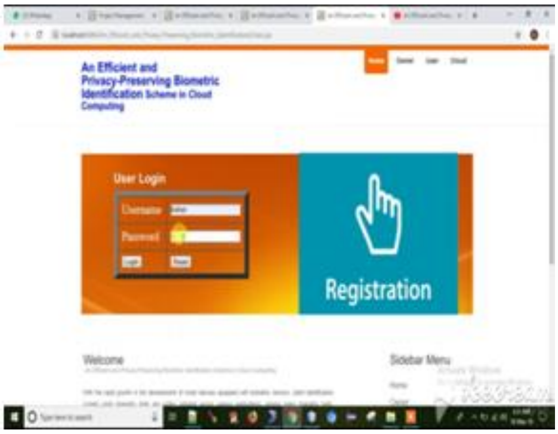


Figure.2. System Architecture

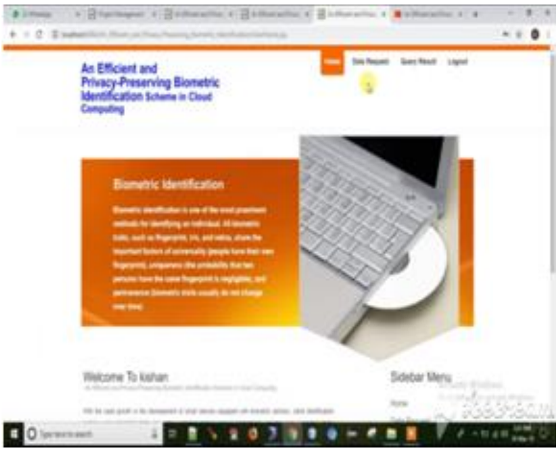
Whenever the new user wants to access the Cloud the first thing he must do is to register by using his fingerprints. Once he is registered he becomes a valid user and can login to the cloud. The fingerprint image is then stored and encrypted using the Reverse Circle Cipher algorithm. The feature extraction is performed on encrypted data. It takes the mean of all the blocks from Reverse Circle Cipher algorithm. This mean is compared with the mean of the data that is already stored in the database while registration. This process of matching is done using a Pearson's formula. It finds the correlation between the two images and gives the result whether he is a valid user or not. Pearson algorithm gives value ranging from -1 to 1. If the value comes closer to 1 than the two images are considered same and user is considered authenticated and allowed login to the cloud.

V. RESULTS

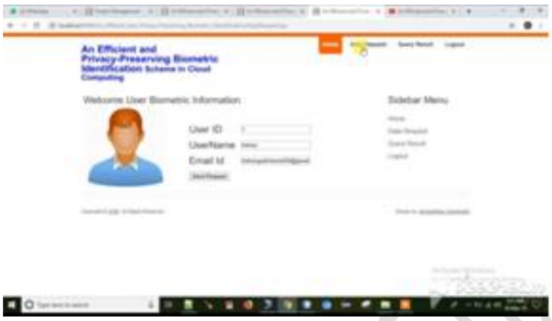
LOGIN PAGE

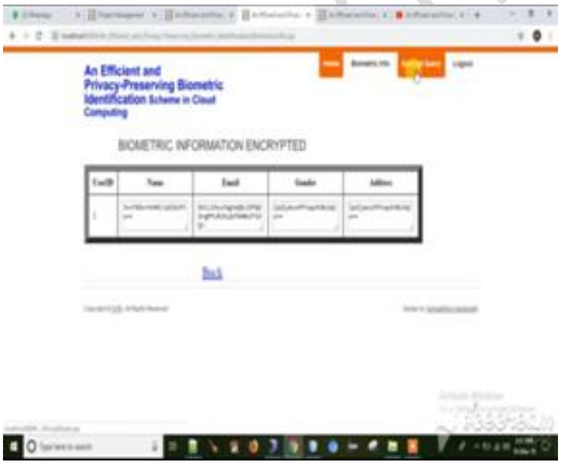

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

BIO-METRIC INFORMATION



WELCOME TO USER BIOMETRIC INFORMATION




An Efficient and
Privacy-Preserving Biometric
Identification Scheme in Cloud
Computing
Home
Biometric Info
Logout
BIOMETRIC INFORMATION ENCRYPTED
UserID
Name
Email
Gender
Address
Back

VI. CONCLUSION

The existing systems have technologies that save the whole data on cloud that gives heavy load on the resources which ultimately leads to slow processing. Also the earlier techniques used for matching images fails in matching those images that have orientation change. So, we proposed a biometric authentication mechanism which allows us to provide secure login into cloud server and verifying the user even if the orientation of fingerprint is changed. All this is done by an Out sourceable two party Privacy preserving Biometric Authentication method. This reduces the threat of data theft and reduces the load on resources.

REFERENCES

[1] Chandra ShekharVorugunti, "A Secure and efficient Biometric Authentication as a service for cloud computing," IEEE, October 09-11 2014.

[2] D. J. Craft "A fast hardware data compression and some algorithmic extensions," IBM J. RES. DEVELOP. VOL. 42 NO. 6 NOVEMBER 1998 .

[3] Cong Li, Zhenzhou Ji, Fei Gu "Efficient parallel Design foe BWTBased DNA Sequence Data Multi-compression Algorithm," Harbin Institute of technology,150001, Harbin, China.

[4] Kiran Kumar K, K.B Raja, "Hybrid Fingerprint Matching using Block filter and strength factor," Second International Conference on Computer Engineering and Applications,2010.

[5] Mr.Jeff Collier, "CIRRUS : Increased Image Dissemination Speed using Cloud resources," 978-1-4673-7565-8/15,2015 IEEE .

[6] Hu Chun, Feng Li "Outsourceable two party privacy preserving biometric authentication," June 4–6, 2014, Kyoto, Japan.

[7] Surender Sharma and Venki Balasubramanian"A Biometric Based Authentication and Encryption framework for sensor Health Data in Cloud ,"2014 IEEE.

[8] Krishnaraj Madhavji Sunjiv Soyjaudah, "Cloud Computing Authentication Using Cancellable Biometrics,"2013,IEEE.

[9] Dr.Anandhakumar P. and Ms. D. Preetha Evangeline, "An Effective Mechanism for Storing Photo Albums on Cloud Storage," 2015 IEEE.

[10] Abdullah A. Albahdal and Terrance E. Bould "Problems and Promises of using the Cloud and

Biometrics," 11th International conference on Information Technology: New Generations,2014.

[11] Dasaradha Ramaiah K and T Venugopal "A novel approach to detect most effective compression Technique Based on Compression Ratio and time
complexity with huge data Load for Cloud Migration," IEEE 2016.

[12] Ms D Preetha, Cephas Paul Edward V and Dr. Anandh Kumar P "An Efficient Mechanism for storing Photo Album on Cloud Storage," IEEE 2015.

[13] Jaime Moreno and Xavier Otazu "image Compression Algorithm Based on Hilber Scanning of Embedded Quadtrees: An Introduction of the Hi-Set Coder," IEEE 2011.

[14] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," in Proceedings of the 16th European conference on Research in computer security, ser. ESORICS'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 190–209.

[15] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," PATTERN RECOGNITION, vol. 35, pp. 861–874, 2001.

AUTHOR'S PROFILE:

[1]. **KORRA PRIYANKA,** Pursuing *M.Tech in CSE* **at** Scient Institute Of Technology, Ibrahimpatnam, Rangareddy, T.S.

[2]. **M.NARENDHAR,** He pursued his B.Tech in CSIT from JNT University Hyderabad, M.Tech Software Engineering from JNT University Hyderabad, Ph.D pursuing from JNT University Hyderabad. He is currently working as Assoc Prof & HOD in Department of CSE at Scient Institute of Technology Ibrahimpatnam. He has 14 years of Academic experience. His research areas include Software Engineering and Data mining. He is a professional member in Computer Society of India. He has published 10 international journals and participated in One International Conference.He Attended and Conduted Many Workshops in different areas.