ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

A Novel Privacy Preserving Biometric Identification Scheme in Cloud Computing

Dharani[1], Lakshmi Priya[2], Nagajothi[3]

Associate Professor, Dept. of IT, PIT, Chennai, India[1]

Student, Dept. of IT, PIT, Chennai, India[2]

Student, Dept. of IT, PIT, Chennai, India [3]

ABSTRACT: In this digital world, people do all their transactions in smart phones itself. No one is ready to spend their time for waiting in a long queue for their work to be done. People depend on online transaction rather than direct deposit. Even though the security is less they prefer only the online transaction. Because the lifestyle of the people is changed and they are living in the digitalized world. Many banking applications are existing but still some of them having its own disadvantages. To provide more security and efficiency in transactions we are developing a banking application and also we are proposing a privacy preserving biometric data in cloud computing .So that bank transactions are made more simple and safe using one individual's biometric data.

KEYWORDS: Banking Application, Face & Iris Recognition, Fingerprint Recognition, Fuzzy logic, KNN Algorithm, Data Server, Bank server, Verification.

I. INTRODUCTION

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

II. LITERATURE SURVEY

Cloud BI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the cloud
A new privacy-preserving biometric identification protocols was implemented, which reduces the computation burden on the database owner. Those protocols are build on new biometric data encryption, distance-computation and matching algorithms that novely exploit the structures of biometric data and properties of identification operations. A complete security analysis shows that their solutions are practically-secure, and they became ultimate solution for a high level privacy protection for a biometric identification outsourcing. They evaluated their protocols by implementing an efficient privacy-preserving fingerprint-identification system, showing that their protocols meet both the security and efficiency. Thus they are used in various privacy-preserving biometric identification applications.

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. EXISTING SYSTEM

A. Traditional Authentication
During transaction, authenticated users should be verified to complete their transaction. To verify user (authenticated user/not) Traditional authentication method was followed. Based on the request, the Data Server will send either passwords or OTP only for requested user. When the user enters correct password or OTP sent by the Data Server then, he is said to be an Authenticated User and his transaction will be successful. If he fails, to enter correct password or OTP then he is said to be an unauthenticated user and he won't be able to continue his transaction to next stage. In this way Traditional authentication occurs.

B. Biometric Authentication
Recent days, Biometric concept became more famous and it was said as more reliable, safe, convenient and secure. So, biometric identification was introduced in bank transactions. During registration process, the users are asked to submit their biometric data. i.e., Fingerprint. All those data will be stored in cloud. Depending upon the users request for transaction, their fingerprints will be scanned and it will be analyzed. When their fingerprints are matched with the data stored in the cloud, then they are said to be authenticated user and his transaction will be successful. If the fingerprints does not match with the data stored in the cloud, then he is said to be an unauthenticated user and he will not be able to proceed his transaction.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

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. To preserve the privacy of biometric data, the biometric data has to be encrypted before outsourcing. Whenever a FBI's partner 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.). The FBI encrypts the query and submits it to the cloud to find the close match.

Disadvantages

- Designing a protocol is a challenging task.
- Fails to satisfy efficiency.
- More computational cost.
- More storage cost.

IV. PROPOSED SYSTEM

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.

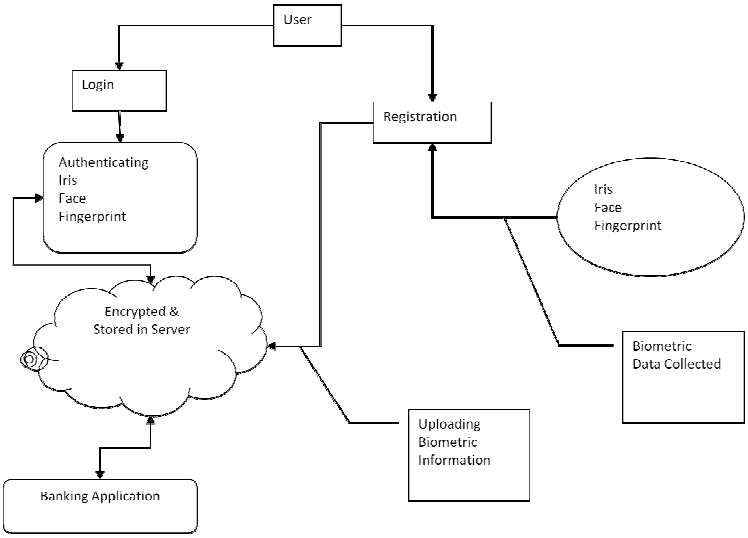

Fig.1 Architecture diagram for the proposed system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

V. WORKING FLOW

First, the users who are interested to use this Banking Application must register their basic details like name, address, email id, phone number and also the user want to create their own password through Bank Server in the Data Server. Immediately Bank server will check whether the details are already Present in the Data Server. If the details are already present in the Data Server then it will sent Acknowledgement message like "Already Exists" otherwise it will store the details in the Data Server and send Acknowledgement Message like "Registered Successfully" to the requested user.

Then, the user has to register in the banking application by filling basic details along with his account number, IFSC code, Micr code. For user's second level secure authentication, the user are asked to register their biometric sample like fingerprint, face and iris patterns. All these data will be stored in Bank Server.

When user wish to do online transaction, based on the previous transaction and range of requested amount the transaction will be classified into three categories such as New Transaction, Normal Transaction and Abnormal Transaction using Fuzzy logic. The Bank Server will search in the database.

- New Transaction means, the user is first time transferring money to new account, then the bank server will ask all three biometric data to verify either the user is authenticated user or not.

- Normal Transaction means, the user already sent money to the person in the certain range of Amount then the user want to send money for the same person with in the rang that transaction is known as Normal Transaction, then the bank server will verify the user with any one biometric data for checking authentication.

- Abnormal Transaction means, it is similar to Normal transaction but the Amount user want to send is higher than the rang , then the bank server will ask on spot any two combination of biometric data to verify authenticated user.

When user chooses their own preference of transactions, for that transaction any combination of biometric data will be scanned and collected samples will be analyzed and validated. When the scanned information matches with the Data Server, then the transaction will be successful otherwise the transaction will be cancelled.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

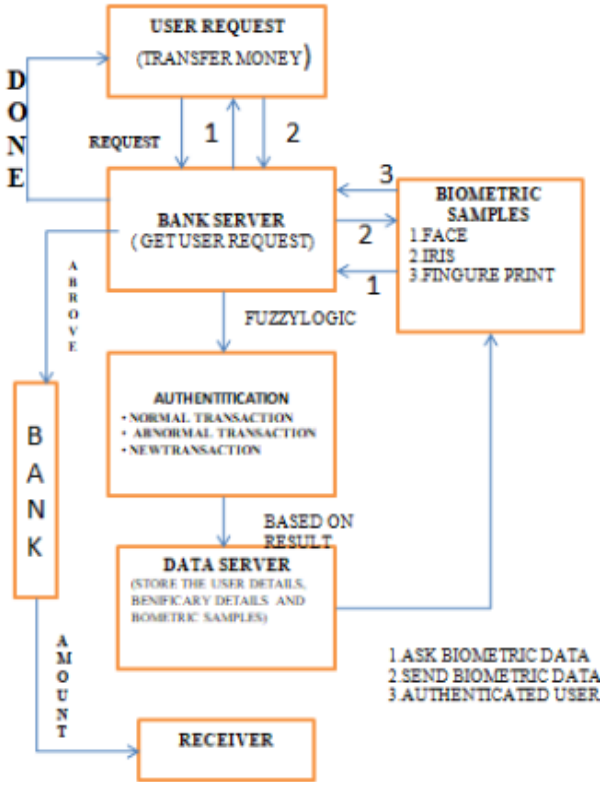

Fig .2 Working flow

VI. ALGORITHM

Initially, New user want to register their personal details and beneficiary details and also their Biometric Samples in the Data server. When the request is received by Bank Server then it will check whether those details are already present in the Data server or not.

After the Registration is done, the Bank server will send an Acknowledgement Email to the registered Email ID that Mail will contain UserID(account number) and password. During First level of Registration user want to create their own Password for their further security.

Step 1: The user sends request to the bank server in order to transfer money to recipient.
Step 2: Data sever receives the request from the user.
Step 3: Transaction is divided into three type using Fuzzy logic.
Step 4: Data Server ask the Biometric Data from user for authentication purpose based on the result of step 3.
Step 5: After the verification the transaction will be done successfully.
Step 6: Stop.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

VII. CONCLUSION

Most of the banking application helps the people to easily complete their task like online shopping, online Ticket booking, etc.. But still some of the banking applications has its own disadvantages. So, bank fraud is also getting increased and hackers also getting benefited. To overcome such problems, a transaction should be made more safe, secure, efficient and comfort in banking application. Our project surely satisfies all these criteria.

REFERENCES

[1]. C. Zhang, L. Zhu and C. Xu, "PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud," Information Sciences, vol. 409, pp. 56-67, 2017.
[2]. 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.
[3]. Q. Wang, S. Hu, K. Ren, et al., "CloudBI: Practical privacy-preserving out- sourcing of biometric identification in the cloud," in European Symposium on Research in Computer Security, pp. 186-205, 2015.
[4]. 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
[5]. Z. Wang, Y. Zhu, and J. Wang, "Collusion-resisting secure nearest neighbour query over encrypted data in cloud," In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on, pp. 1-6, 2016.
[6]. W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulisa, ``Secure kNN computation on encrypted databases,&#39;&#39; in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2009, pp. 139_152. A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, ``Filterbank- based _ngerprint matching," IEEE Trans. Image Process., vol. 9, no. 5, pp. 846_859, May 2000.
[7]. H. Delfs, H. Knebl, and H. Knebl, Introduction to Cryptography. Berlin, Germany: Springer, 2002.
[8]. K. Liu, C. Giannella, and H. Kargupta, ``An attacker's view of distance preserving maps for privacy preserving data mining," in Knowledge Discovery in Databases: PKDD (Lecture Notes in Computer Science). Heidelberg, Germany: Springer, 2006, pp. 297_308.
[9]. Y. Wang and D. Hatzinakos, ``Face recognition with enhanced privacy protection," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Apr. 2009, pp. 885_888.
[10]. K.-S. Wong and M.-H. Kim, ``A privacy-preserving biometric matching protocol for iris codes veri_cation," in Proc. 3rd FTRA Int. Conf. Mobile, Ubiquitous, Intell. Comput. (MUSIC), Jun. 2012, pp. 120_125.
[11]. Y. Xiao et al., ``A survey of key management schemes in wireless sensor networks," Comput. Commun., vol. 30, nos. 11_12, pp. 2314_2341, Sep. 2007.
[12]. X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, ``An effective key management scheme for heterogeneous sensor networks," Ad Hoc Netw., vol. 5, no. 1, pp. 24_34, 2007.