An Efficient Biometric Identification System

[1]Mr.Satish Manje, [2]Miss.Tejashree Wagh, [3]Miss.Pratiksha Bhavsar, [4]Miss.Amrita Nath

[1]Asst.Professor,[2,3,4]UGStudent,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

[1]satishmanje93@gmail.com, [2]waghtejashree@gmail.com, [3]pratikshabhavsar1997@gmail.com, [4]amrita1998nath@gmail.com

Abstract- Biometric identification scheme has been in huge demand since it provides a reliable way to identify the users. An efficient biometric identification outsourcing scheme which is privacy preserved specifically on biometric data, is proposed. The biometric data is encrypted and outsourced to the cloud server is present here. The owner of database encrypts the query data and then send it to cloud, in order to execute identification process. Then the cloud performs identification operations over the encrypted database and returns the result to the database owner. A security analysis is carried out, indicates the proposed scheme is secure even. Even if the attackers can forge identification requests and collude with the cloud. As compared to previous systems, results show the proposed system leads to a better performance in preparation as well as identification procedures to be the other biometric data which is kept hidden from the service provider of cloud.

Keywords- biometric identification; efficient scheme; identification process; cloud computing

I. INTRODUCTION

Biometric identification scheme has been in huge demand since it provides a reliable way to identify the users. As compared to the old authentication methods such as pins, passwords and identity cards, a biometric identification is considered to be more trustworthy and convenient. A biometric identification has been used widely in numerous fields, which uses the biometric traits such as fingerprint [2], iris [3], and facial patterns [4], which can be identified as well as collected from various sensors [5]-[9]. In a biometric identification scheme, the owner of the database, consider a FBI who is responsible to look over and manage the fingerprints database of entire nation, can desire to leak or outsource the huge biometric data to the cloud server (e.g., Flipkart) to get rid of the computation costs and expensive storage. However, to preserve and prevent the privacy of this biometric data, this data has to be encrypted before outsourcing it to the cloud. Whenever a outsider wants to verify an individual's actual identity, the outsider turns to the FBI and then creates a query for identification of individual, with the help of the biometric traits such as fingerprint, iris, voice pattern, facial pattern, etc. Hence, how to design such a system which is a combination of an efficient as well as privacy-preserving biometric identification scheme using cloud computing is a challenging part. Numerous solutions for privacy-preserving biometric identification [10]-[13] have been proposed till date. However, most of these solutions mainly focus on privacy preservation and ignore the efficiency, such as schemes based on homomorphic encryption and oblivious transfer [10], [11] and for fingerprints and face image identification respectively. In a biometric identification scheme, the owner of the database.

II. AIMS AND OBJECTIVE

a) Aim

The basic idea for proposing this system is to provide an biometric identification system which is efficient and privacy-preserving, can resist the any attack caused by the users and the cloud. The data owner encrypts the query data and submits it to the cloud, in order to execute a biometric identification scheme. The cloud conducts process of identification on the encrypted data to return the result to the owner. The exact aim is to secure the system even in case attackers forge identification requests and tries to collude with the cloud.

b) Objective

Security and efficiency both are considered in the proposed scheme, in order to achieve practicality.

- **Efficiency:** Computational cost must be as minimum as possible at user side as well as owner side, in order to obtain more efficiency
- **Security:** The privacy of data consisting biometric traits of the clients must be protected. Attackers or others should not learn anything regarding the confidential information.
- **Biometric Encryption:** When applied on biometric database, even if cryptography is reliable, it falls in

DOI : 10.35291/2454-9150.2020.0239

the inadequate category. Depending on the cryptographic mechanisms it is inadequate.

- **Anonymous Database:** The aim is to verify anonymous data consisting the membership of the user by not even knowing his/her actual identity. The main question here is whether in anonymous data there's need for security between two components: The client and the cloud server.

III. LITERATURE SURVEY

1)Julien Bringer, HerveChabanne and Bruno Kindarji. "Identification with encrypted biometric data"

Biometrics made identification of human possible using a sample of their biometric trait with associated database. Traditional identification techniques take us to concerns regarding privacy. This is a new scheme to authenticate someone using biometric traits in an encrypted way.

2) Joaquim de MiraJr.Hugo Vieira NetoEmailauthorEduardo B. NevesFábio K. Schneider. "Biometric-oriented Iris Identification Based on Mathematical Morphology".

A new system for identification of human irises is presented in this scheme. This system depends on morphological image processing used for the identification of various skeletons of iris structures, those are later used for extraction of features.

3) Changhee Hahn JunbeomHur. "Efficient and privacy-preserving biometric identification"

With the increasing rate in the development of smart equipment associated with biometric sensors, identification using biometric traits are very commonly adopted across different applications. Among all the biometric traits, the fingerprint identification based systems have been mostly learned and deployed.

IV. EXISTING SYSTEM

This is privacy preserving protocol for finger print-based authentication. Let us assume a scenario where a user is equipped with a fingerprint reader and is interested into peeking, if the associated fingerprint belongs to the database of entities which are authorized and managed by a server. For privacy, it is needed that the user learns nothing from the database and the server must not get any kind of information about the biometry asked, and the output of the identification process. The proposed scheme follows an approach that is multi-party computation approach and makes use of homomorphic encryption as partial cryptographic primitive. To keep the complexity of the system as low as possible, a typical representation of fingerprint images, named Finger code, is adopted.

V. COMPARTIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	METHOD	ADVANTAGE	DISADVANTAGE
1.	An efficient and privacy-preserving biometric identification scheme in cloud computing	Liehuang Zhu, Chuan Zhang, Chang Xu, Ximeng Liu, Cheng Huang.	Encryption and decryption of biometric data using cipher text in cloud computing.	It has cloud server to store infinity data. It is very inexpensive	
2.	Biometric-oriented iris identification based on mathematical morphology	Joaquim de Mira Jr. , Eduardo B. Neves, Hugo Vieira Neto, Fabio K. Schneider	This technology is based on morphological image processing for the identification of iris	It is includes iris identification, which is more efficient secure and reliable	This system guarantees the optimization but time complexity is still an issue.
3.	Efficient and privacy-preserving biometric identification [17]	Changhee Hahn, JunbeonHur	Symmetric homomorphic encryption	It is faster than the existing scheme.	It has expensive storage and computation cost is high
4	Efficient and privacy-preserving face recognition	Ahmad-Reza Sadeghi, Thomos Schneider, ImmoWehrenberg	Cryptographic building blocks combining homomorphic encryption with garbled circuits.	It consumes less computation complexity.	It has expensive storage and computation cost is high.

VI. PROBLEM STATEMENT

This system reduced the cost and made it cost-efficient. Since cloud computing is used in this project, memory is major portion which is covered and saved. The data is stored in encrypted form so even in the case of leakage the data cannot be misused. This project also focuses on the time complexity issue.

VII. PROPOSED SYSTEM

In this system, here it is shown that an efficient and privacy protecting biometric identification system which can resist any collusion attack held by the clients and the cloud. Especially, main aspects can be summarized as follows:

• In this system, it is checked whether the identification system exposes its own insufficiencies and weakness

DOI : 10.35291/2454-9150.2020.0239

under the proposed level-3 attack of security. Especially, it proposes that the attacker can recover the private keys by collusion with the cloud, and hence decrypt each user's biometric traits.

- This is a novel system based on efficient and privacy preserving biometric identification. The deep analysis on security shows that the proposed system can achieve a mandatory level of protection. Most importantly, this system is safe under the biometric identification output model and also resists the attack which is proposed.

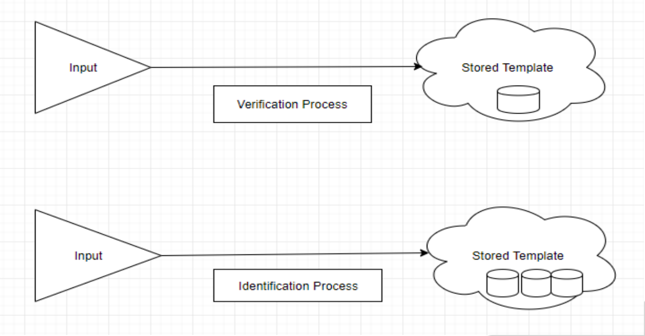


Fig.1: Proposed system

VIII. ALGORITHM

NOVEL BIOMETRIC IDENTIFICATION SCHEME ALGORITHM:

This algorithm is divided into two steps as follows:

STEP 1: Preparation process

- **Cipher text Policy Attributes Based Encryption Algorithm**

Input: plaintext message M

Output: Cipher text.

Preparation:

1.Select a random number r in p–integer modulo Z with the polynomial function and sets q(R,0)=r.

2.q(x,0)=q(parent node(x, index)) for intermediate nodes.

3. Let L be the set of leaf nodes in access tree structure, then the cipher text is generated based on the given access tree structure T as:

Ciphertext (C) = {Fill_AccessTree(Policies, s Є Zr ,PUK), for all x Є X:Cx =kq(x,0), C1x = H(A(x))q(x,0) , m.o,h Є PUK} Є PUK}

STEP 2: Identification process

- **Euclidean-Distance Protocol Algorithm**

Input to the server: a matrix {v i, j} M×N.

Input to the client: a vector v ′ = [v1', ... ,vN'].

Output of the server: M random integers [d1',...,dM'],

where di' = di' +ri .

Output of the client: M integers [r1,...,rM].

Preparation:

1.Client chooses[r1,…,rM], and computes [d']=[d1' || d2'‖….‖dM']

2. Send [d1' || d2'‖….‖dM']

3. The server decrypts to get [d1',….,dM']

4. The server generates a key pair ⟨pkS,skS⟩.

5. For 1 ≤ j ≤ N, the server computes [2c j] pkS.

IX. MATHEMATICAL MODEL

PREPARATION PROCESS :

In the preparation process, bi is the i-th sample feature vector derived from the fingerprint image using a feature extraction algorithm. To be more exact, bi is a non-dimensional vector which consists of l bit each element and where n = 640 and l = 8. For easy identification, bi is increased by adding an (n + 1) th element of Bi. After which, the owner of database encrypts Bi with the private key M1 as follows:
Ci = Bi × M1……………….. [9]
The owner of database later performs the following operation:
Ch = M −1 2 × H T…………[10]
Every Finger Code Bi is adjoint with an index Ii. After execution, the encryption operations, the owner of database then stores (Ci, Ch, Ii) to the cloud.

X. SYSTEM ARCHITECTURE

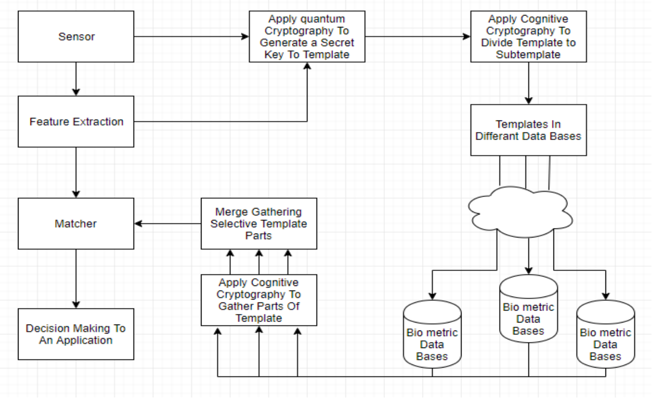

Sensor
Apply quantum Cryptography To Generate a Secret Key To Template
Apply Cognitive Cryptography To Divide Template to Subtemplate
Feature Extraction
Templates In Differant Data Bases
Matcher
Merge Gathering Selective Template Parts
Apply Cognitive Cryptography To Gather Parts Of Template
Decision Making To An Application
Bio metric Data Bases
Bio metric Data Bases
Bio metric Data Bases

Fig.2: System Architecture

Description: This section introduces the system model, attack model, design goals and the notations used in the following sections. In System Model, there are three types of entities involved in the system including the database owner, users.

XI. ADVANATGES

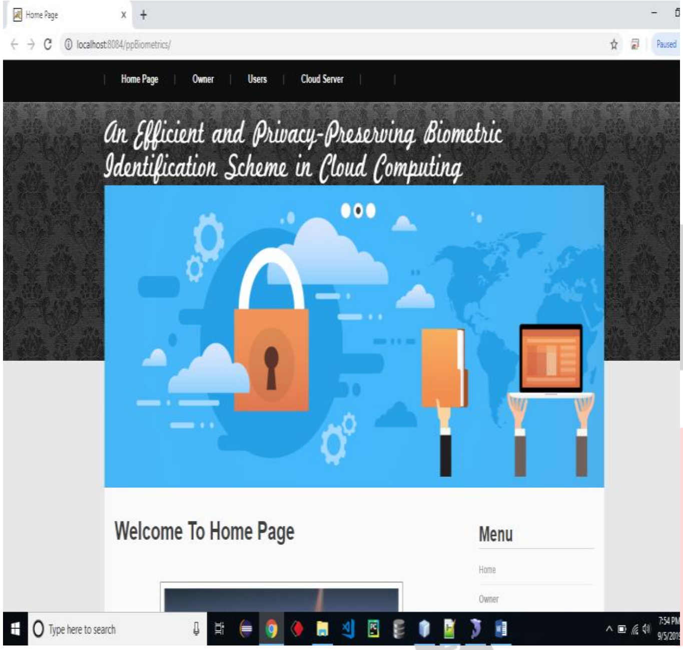
- Biometric identification is a trustworthy and reliable way of identifying individuals.
- The worldwide adoption of this biometric identification needs very strong privacy and protection

DOI : 10.35291/2454-9150.2020.0239

against possible attacks, loss, or misuses of biometric data.

- The traditional techniques for this efficient biometric identification system firstly depend on the conventional cryptographic primitives like the oblivious transfer and homomorphic encryption, which obviously introduce very high cost to the system and are not considerable.
- With the increasing growth in biometric sensors, the user identification system with biometric traits is very vastly accepted across many applications.

XII. DESIGN DETAILS



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

Welcome To Home Page

Fig 3: Result

XIII. CONCLUSION

Thus we have tried to implement the paper “Liehuang Zhu, Chuan Zhang, Chang Xu, Ximeng Liu, Cheng Huang, “An efficient and privacy-preserving biometric identification scheme in cloud computing,” -IEEE Access 2018. In this paper an efficient and privacy-preserving biometric identification system using the cloud computing is been proposed. The detailed analysis shows it can resist the potential attacks. Besides, through performance evaluations, the proposed scheme meets the efficiency needs as well.

REFERENCE

[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,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 onim plant able medical devices,”inProc.ofIEEEGLOBECOM2010,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),2010IEEESymposiumon,pp. 239-254, 2010.

[12]D.Evans,Y.Huang,J.Katz,etal.,“Efficientprivacy-preservingbiometric identification,” in Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS, 2011.

[13]J. Yuanand S. Yu,“ Efficient privacy-preserving biometric identification in cloud computing,” inProc. Of IEEEINFOCOM203.

[14]Q.Wang,S.Hu,K.Ren,etal.,“CloudBI:Practicalprivacy-preservingoutsourcing of biometric identification in the cloud,”in Computer Security, pp. 186-205, 2015.