VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belgaum -590014, Karnataka.

PROJECT PHASE 1 REPORT

on

PRIVACY PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING USING BLOCKCHAIN

Submitted by

JYOTHSNA SARAH (1BM15CS135)
AASHREYA REDDY (1BM15CS151)

Under the Guidance of
Prof. Latha NR
Assistant Professor, BMSCE

in partial fulfilment for the award of the degree of
BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING

BMS COLLEGE OF ENGINEERING
(Autonomous Institution under VTU)
BENGALURU-560019

2018-2019

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belgaum -590014, Karnataka.

PROJECT PHASE 1 REPORT

on

PRIVACY PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING USING BLOCKCHAIN

Submitted by

JYOTHSNA SARAH (1BM15CS135)
AASHREYA REDDY (1BM15CS151)

Under the Guidance of
Prof. Latha NR
Assistant Professor, BMSCE

in partial fulfilment for the award of the degree of
BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING

BMS COLLEGE OF ENGINEERING
(Autonomous Institution under VTU)
BENGALURU-560019

2018-2019

B M S College of Engineering,
Bull Temple Road, Bangalore 560019
(Affiliated to Visvesvaraya Technological University, Belgaum)
Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the project work entitled PRIVACY PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING USING BLOCKCHAIN carried out by **JYOTHSNA SARAH (1BM15CS135)** and **AASHREYA REDDY (1BM15CS151)** who are bonafide students of **B M S College of Engineering**. It is in partial fulfilment for the award of **Bachelor of Engineering in Computer Science and Engineering** of the Visveswaraiah Technological University, Belgaum during the year 2018-19. The project report has been approved as it satisfies the academic requirements in respect of **Project Phase 1 (16CS7DCPP1)** work prescribed for the said degree.

Signature of the Guide	Signature of the HOD
Prof. Latha NR	Dr. B G Prasad
Assistant Professor	Prof & Head of Dept of CSE
BMSCE, Bengaluru	BMSCE, Bengaluru

External Viva

Name of the Examiner	Signature with date
1. _____	_____
2. _____	_____

Table of Contents

Abstract

With the birth of electronic banking, e-commerce, and smartcards and an increased emphasis on the privacy and security of information stored in various databases, *automatic* personal identification has become a very important topic. Accurate personal identification is now needed in a wide range of civilian applications involving the use of passports, cellular telephones, automatic teller machines, and driver licenses. The traditional methods of identification [password or personal identification number (PIN)] and token-based (passport, driver license, and ID card) which are knowledge-based are prone to fraud because PIN's may be forgotten or guessed by a hacker and the could be replicated, lost or stolen. Therefore, the need for biometrics showed up. Biometrics tend to be more convenient than other methods of identity authentication. This is because of the uniqueness and permanence of it. You might forget your ID at home when you head out the door, but you'll still be able to use biometric devices. Imagine verifying your identity while at the store by swiping your finger across a sensor.

Traditionally, in cybersecurity anyone wanting to store, share or process information must own it. This involves creating, borrowing or buying that information, obtaining permission to use it (if necessary) and then ensuring everyone is aware of any changes. The earlier methods in verifying & identifying was to gain permission from a user and then subjugate it to different methods of security. All of this would be centralized.

The main objective of the project is to create a biometric scheme that helps store confidential and secure data in a cloud storage system such that the data isn't compromised. The biometric data is highly sensitive and needs to be secured and not easily accessible. This is done using blockchain technology a new and high level security that is implemented.

Blockchain technology has been around for just under a decade, initially introduced as a way to store and/or send the first cryptocurrency, Bitcoin. However, as the technology has gradually spread worldwide, people have begun using it in a variety of ways in numerous industries, including to increase cybersecurity.

Biometric technology works by capturing anatomical or behavioural patterns found in human beings. Everyone's biometric patterns are different and biometric technology can find this minute difference in these patterns using technological, mathematical and statistical means. Biometric recognition technology has proved its superiority over traditional and other recognition methods; however, permanence of human biometric patterns becomes the strength as well as the weakness of this technology. Your fingerprints or iris patterns are unique as well as permanent, it is a good thing when your biometric data is secure, and a very bad thing when it is not.

2. Introduction

2.1 Overview

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 project, we propose an efficient and privacy-preserving bio- metric 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.

2.2 Motivation

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, 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.

2.3 Objective

The main objective of the project is to create a biometric scheme that helps store confidential and secure data in a cloud storage system such that the data isn’t compromised. The biometric data is highly sensitive and needs to be secured and not easily accessible. This is done using blockchain technology a new and high level security that is implemented.

2.4 Scope

Protect biometric features such as fingerprint and iris patters in a secure and preventive from hacks method. Prevent counterfeit government identification. All of these solutions involve identity claims residing on a blockchain to achieve decentralization, executable contracts, secure encryption, and consensus.

2.5 Existing system

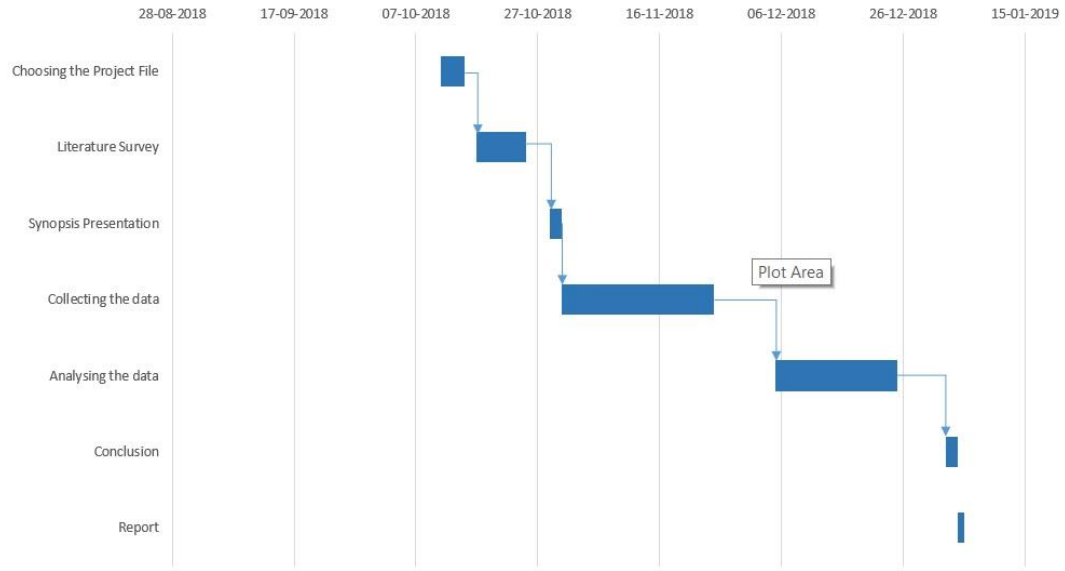
During the identification process, the privacy of biometric data should not be protected. Attackers and the semi-honest cloud should learn all about the sensitive information, there is no security to protect our data.

2.6 Proposed system

We propose an efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users and the cloud. We examine the biometric identification scheme and show it's in sufficiency's 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. In the cloud, the blockchain technology is used which hashes the data and saves it in a decentralized block.

2.7 Work Plan

TASK NAME	DURATION	START DATE	FINISH
Choosing the Project File	4	Thu 11-10-2018	Tue 16/10/18
Literature Survey	8	Wed 17/10/18	Fri 26/10/18
Synopsis Presentation	2	Mon 29/10/18	Tue 30/10/18
Collecting the data	25	Wed 31/10/18	Tue 04/12/18
Analysing the data	20	Wed 05/12/18	Tue 01/01/19
Conclusion	2	Wed 02/01/19	Thu 03/01/19
Report	1	Fri 04/01/19	Fri 04/01/19



3. Literature survey

Traditionally, in cybersecurity anyone wanting to store, share or process information must own it. This involves creating, borrowing or buying that information, obtaining permission to use it (if necessary) and then ensuring everyone is aware of any changes. Biometrics tend to be more convenient than other methods of identity authentication. This is because of the uniqueness and permanence of it. You might forget your ID at home when you head out the door, but you'll still be able to use biometric devices. Imagine verifying your identity while at the store by swiping your finger across a sensor. Blockchain technology has been around for just under a decade, initially introduced as a way to store and/or send the first cryptocurrency, Bitcoin. However, as the technology has gradually spread worldwide, people have begun using it in a variety of ways in numerous industries, including to increase cybersecurity.

Need for Blockchain

The conventional cryptographic techniques for privacy-preserving biometric identification such as homomorphic encryption and oblivious transfer, which inevitably introduce tremendous cost to the system and are not applicable to practical large-scale applications. A novel privacy-preserving biometric identification scheme which achieves efficiency by exploiting the power of cloud computing. Here the biometric database is encrypted and outsourced to the cloud servers. This is our idea of stepping up the traditional method and introducing blockchain technology to it. Blockchain technology is best described as a distributed ledger. It allows multiple nodes on a network to connect and work together to form a decentralized network. The network is capable of self-sustaining without any centralized control or authority, giving it a unique value in our current society. When a transaction takes place between users, it needs to be validated. Consensus algorithm is used to verify an operation across the network. Also, new blocks are created to store the transactions. Once all transactions assigned to a block are verified, the block is added to the existing blockchain. The addition is permanent, and no data can be altered or deleted in any way.

Advantages of Blockchain in Cloud Computing

1. More security
2. Reduce workload and enhance productivity
3. Better flexibility and speed
4. Efficiency: Computational costs should be as low as possible at both the database owner side and the user side. To gain high efficiency, most biometric identification operations should be executed in the cloud.
5. Security: During the identification process, the privacy of biometric data should be protected. Attackers and the semi-honest cloud should learn nothing about the sensitive information.

4. Requirement Analysis and Specification

4.1 Functional Requirements

FR	Description
FR1	Understanding the cryptographic and encryption alogorithms.
FR2	Development of blockchain technology. Understanding of blockchain technology and its implementation.

4.2 Non- functional Requirements

Characteristic	Sub characteristic	Description
Usability	Ease of use	Users can access the data to authenticate the validity of the identity of the person.
Efficiency	Performance	Computational costs should be as low as possible at both the database owner side and the user side. To gain high efficiency, most biometric identification operations should be executed in the cloud.
Security	Access restriction	During the identification process, the privacy of biometric data should be protected. Attackers and the semi-honest cloud should learn nothing about the sensitive information. Access is limited to only those authorized.

4.3 Hardware Requirements (All the below mentioned requirements are from development and testing perspective only)

Feature	Requirement
Processors (CPUs)	Multi-core x64 compatible processors
Memory	8 GB minimum (depending on data volumes, more may be required) Qlik Sense is an in-memory analysis technology. The memory requirements for the Qlik Sense products are directly related to the amount of data being analyzed.
Disk space	5.0 GB total required to install
Storage	A network file share is required for the storage to be accessible by all servers in the site. In case of a single-server deployment, local disk storage may be sufficient. Sufficient storage is required for the volume of apps and content used in the deployment.

4.4 Software Requirements (All the below mentioned requirements are from development and testing perspective only)

Feature	Requirement
Platforms	4.5 Microsoft Windows 7 (64-bit version only) 4.6 Microsoft Windows 8.1 (64-bit version only) 4.7 Microsoft Windows 10 (64-bit version only)
Coding Language	Java (JDK 1.7)
Web Technology	Servlet, JSP
IDE	Eclipse Galileo
Database	My-SQL 5.0
JDBC Connection	Type 4 Driver

5. Design

5.1 High level Architecture:

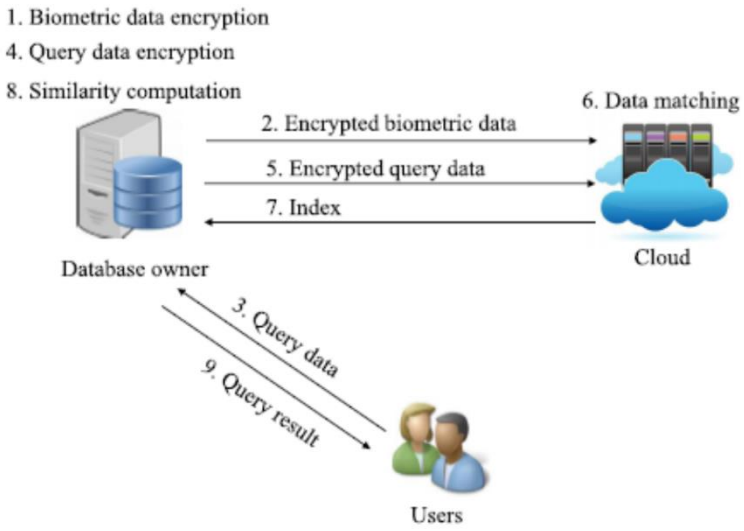
Three types of entities are involved in the system i.e. the database owner, users and the decentralized cloud. The database owner holds a large size of biometric data which is encrypted and transmitted to the cloud for storage. In the cloud, a block is created for each user which contains the encrypted data, generating a hash code which is encrypted and stored in different nodes.

Back End:

This is where the data is handled. The biometric data is first encrypted using the encryption algorithm in the database. The data is then sent to the cloud which uses the block chain technology to hash the data and secure it in a decentralised manner.

Front End:

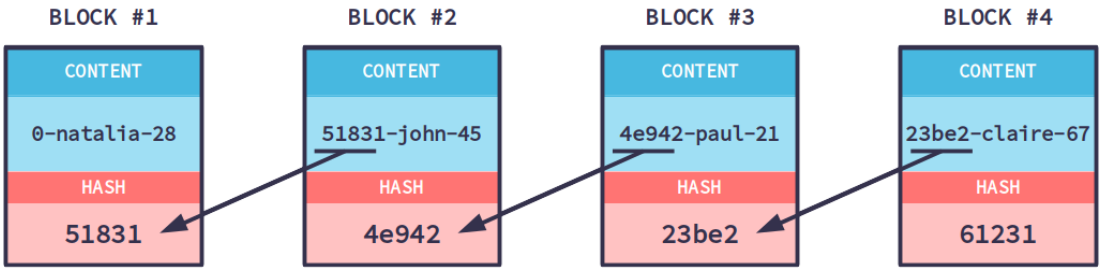
The Front End is where end users interact with the documents and data that is available for them. They are able to authenticate the data that is present to them. The end user requests the data from the database and can view only the queried data.



(Fig 3.1: System Architecture)

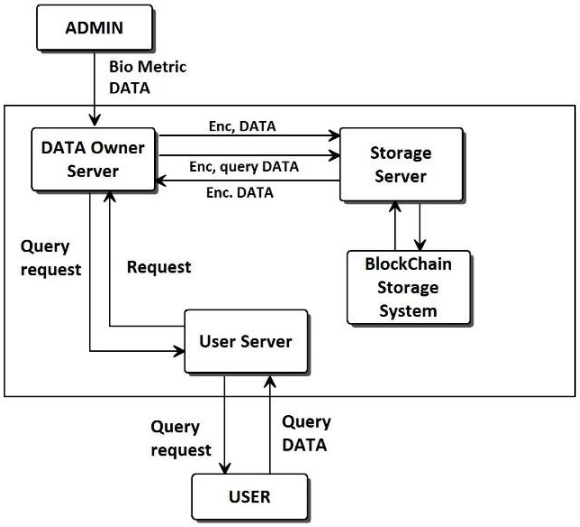
Blockchain architecture:

A blockchain is a database that is shared over a network of computers. Once a record has been added to the database it is very difficult to change. To ensure all the copies of a database are the same, a network makes constant checks. The blockchain technology uses a mathematical function called Hash which turns data into a 64-character long code. The hash code identifies the block in the blockchain and protects its content. Even the addition of a space or a blank line or change a letter to the capital letter can change completely the hash of the output code. Every block must have an identification code: this code will be calculated with the hash.



(Fig 3.2: Blockchain)

In order to build a chain of blocks you must link each block to its previous one: so a block must contain the identification code of the previous block. Changing the content of the block will result in the change of the hash of the block too. The change of the content of the block not only invalidates the block itself but causes the invalidation of all the following blocks.



(Fig 3.3: High level design)

5.2 Methodology:

When a user wants to identify him / her, a query request is being sent to the database owner. After receiving the request, the database owner generates a cipher text for the biometric trait and then transmits the cipher text to the cloud for identification. The cloud server figures out the best match for the encrypted query and returns the related index to the database owner. Finally, the database owner computes the similarity between the query data and the biometric data associated with the index, and returns the query result to the user.

6. Conclusion

The previous works of privacy preserving biometric identification scheme in cloud shows a traditional approach to biometrics which only include the fingerprints of the individual. Fingerprint verification & identification is one of the first biometric approaches that came into existence. But along with convenience and security comes a concern for privacy. For biometrics to work, there needs to be a database containing the relevant information for everyone authorized by the system. The need for a secure storage of biometric thus began. it. The idea behind blockchain is simple. It is designed to be immutable, tamper proof, and democratic. Blockchain is still an emerging technology and evolving with each passing day. Most security vulnerabilities are patched up quickly, and in extreme cases, they can result in a new version of that blockchain known as a hard fork. Blockchain is a much better solution to storing and exchanging digital value than anything that has come before it.

7. References

1. Feature Level Fusion Using Hand and Face Biometrics by Arun Rossa and Rohin Govindarajanb
2. Biometric-oriented Iris Identification Based on Mathematical Morphology by Joaquim de Mira Jr. , Hugo Vieira Neto , Eduardo B. Neves , F´abio K. Schneider
3. Face Identification by Fitting a 3D Morphable Model using Linear Shape and Texture Error Functions by Sami Romdhani, Volker Blanz, and Thomas Vetter**,** University of Freiburg, Germany
4. Efficient Privacy-Preserving Biometric Identification in Cloud Computing by Jiawei Yuan and Shucheng Yu, University of Arkansas at Little Rock, USA
5. Filterbank-Based Fingerprint Matching by Anil K. Jain, *Fellow, IEEE*, Salil Prabhakar, Lin Hong, and Sharath Pankanti, IEEE 2000
6. Biometric-based authentication and blockchain storage for self-sovereign identity systems by J.S. Hammudoglu, J. Sparreboom, J.I. Rauhamaa, J.K. Faber, L.C. Guerchi, I.P. Samiotis, S.P. Rao and J.A. Pouwelse (course supervisor), Computer Science department, Delft University of Technology, The Netherlands., 2017
7. Identity Management in the Age of Blockchain 3.0 Arthi Manohar
8. Backing Rich Credentials with a Blockchain PKI∗ Karen Lewison and Francisco Corella October 24, 2016
9. A Method for Decentralized Biometric-based Self-Sovereign Identity by Asem Othman and John Callahan ,2017
10. Blockchain-based Identity Management with Mobile Device Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi Department of Computer Science, University of Houston Houston, Texas
11. A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain Montes D. Juan, Rincón P. Andrés, Páez M. Rafael, Ramírez E. Gustavo, and Pérez C. Manuel I

12. Fingernail analysis management system using microscopy sensor and blockchain technology Shih Hsiung Lee and Chu Sing Yang, International Journal of Distributed Sensor Networks, 2018

13. Decentralized Biometrix Signing of Digital Contracts by Anthony M. Butler, Ghada Dulaim , Victor Usobiaga, International Business Machines Corporation , 2017