Dissertation Title:

Efficient and Privacy Preserving Biometric Identification Scheme in Cloud Computing

Course No: SS ZG628T
Course Title: Dissertation

Dissertation Work Done by:

Student Name: Manam Bharadwaj

BITS ID: 2021MT13176

Degree Program: Master's in Software Systems

Research Area: Cloud & Enterprise security

Dissertation Work carried out at:

Dassault Systemes, Bengaluru

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE
PILANI
VIDYA VIHAR, PILANI, RAJASTHAN - 333031.
July 2023

Abstract

Keywords: Biometric identification, cloud-based services, privacy preservation, encryption mechanism, secure communication protocols, efficient cloud matching, scalability, false positives, false negatives, user-friendly interface, database owner, collusion attacks, secure biometric identification, cloud computing.

This research endeavors to develop a robust and secure biometric identification scheme tailored for cloud-based services, in response to the growing demand for robust authentication mechanisms in the era of cloud computing and the storage of sensitive data. The proposed system focuses on privacy preservation by employing encryption techniques to safeguard biometric data before transmitting it to the cloud, ensuring the confidentiality of user traits such as fingerprints, iris, and facial patterns.

The research objectives encompass several critical aspects. Firstly, an effective encryption mechanism will be devised to protect biometric data both during transmission and while stored in the cloud. Privacy-preserving techniques will also be implemented to thwart unauthorized access to users' biometric traits. Secure communication protocols will be integrated to prevent eavesdropping and unauthorized access during the identification process.

The efficiency of cloud matching is crucial to process encrypted queries and locate the best match among encrypted biometric data, optimizing computation time and resource utilization. The system will prioritize accuracy and reliability, aiming to minimize false positives and false negatives during user identification. Moreover, the system's scalability will be evaluated to ensure top-notch performance under heavy workloads and a large number of users and biometric datasets. A user-friendly interface will be designed to facilitate seamless interactions, enabling users to initiate identification requests effortlessly and retrieve prompt results.

By providing a reliable and privacy-preserving solution for personal identification, this project aims to advance secure biometric identification in cloud computing. Rigorous analysis and experimentation will evaluate the efficiency and effectiveness of the proposed scheme, contributing significantly to the improvement of biometric identification systems in the cloud.

Contents

Problem Statement:

The problem at hand is to develop and implement an efficient and secure biometric authentication system for cloud-based services. With the increasing reliance on cloud computing and the proliferation of sensitive data stored in the cloud, there is a growing need for robust and reliable authentication mechanisms to protect user accounts and sensitive information from unauthorized access.

In July 2018 telecom regulatory authority of India (TRAI) chairman R.S Sharma post is author no in twitter and challenges author critics to do him harm if they could. Within 7 hours ethical hackers posted screenshot of sending re.1 to Sharma via the Aadhaar enabled service and also, they published 14 items, which includes Sharma's mobile no DOB, residential address, phone no, PAN no, Bank details, etc. As of now our Aadhaar card data are not safely stored in cloud by govt. of India, which create a big problem to our privacy.

Background:

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, 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. 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.

Objective:

The key objectives are as follows:

1. Efficient Biometric Encryption: Develop an efficient and robust encryption mechanism for biometric data to ensure that sensitive information remains secure during transmission and storage in the cloud.
2. Privacy Preservation: Design privacy-preserving techniques to protect the confidentiality of users' biometric traits, ensuring that unauthorized parties, including the cloud service provider, cannot access or infer personal information from the stored data.
3. Secure Data Transmission: Implement secure communication protocols between the database owner, users, and the cloud to prevent eavesdropping and unauthorized access to sensitive data during the identification process.
4. Efficient Cloud Matching: Optimize the cloud's matching algorithm to efficiently process the encrypted queries and find the best match among the encrypted biometric data, reducing computation time and resource overhead.
5. Accuracy and Reliability: Ensure that the biometric identification system maintains a high level of accuracy and reliability in identifying users, minimizing false positives and false negatives.
6. Scalability and Performance: Evaluate the system's scalability to handle a large number of users

and biometric data sets while maintaining high-performance levels even under heavy workloads.
7. Usability and User-Friendly Interface: Design a user-friendly interface that allows seamless interactions between users and the system, making it easy for individuals to initiate identification requests and receive results promptly.

By achieving these objectives, the proposed system aims to contribute significantly to the field of biometric identification in cloud computing, providing an advanced and secure solution that respects users' privacy and withstands potential security threats.

Scope of Work:

The proposed system aims to develop a secure and efficient biometric identification system that safeguards user privacy and resists collusion attacks from both users and the cloud. Previous research in authentication security systems has been analyzed, revealing weaknesses that the proposed scheme aims to overcome.

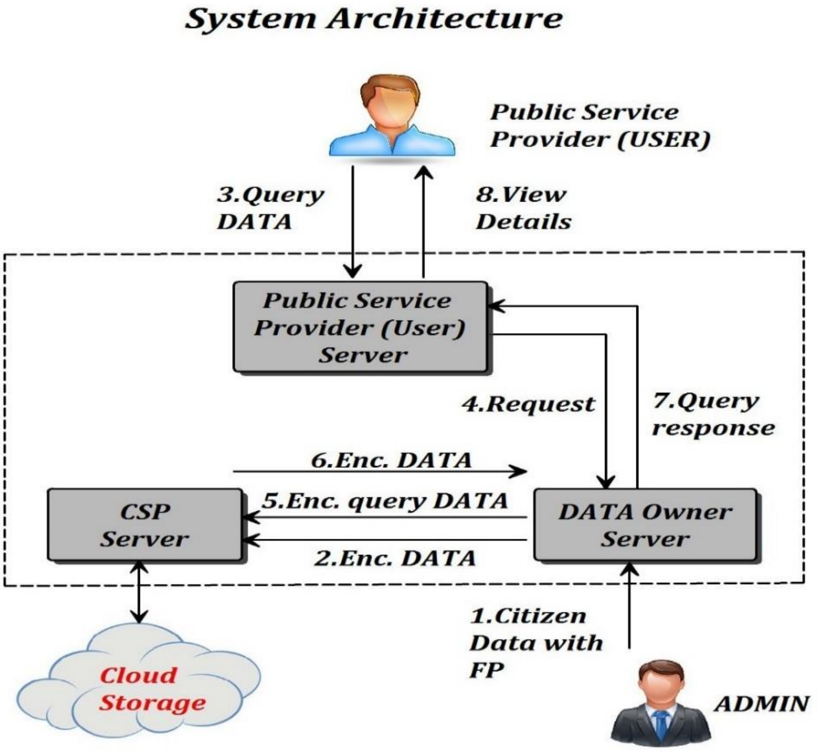


Fig 1: System Architecture

The system involves three main entities: the database owner, users, and the cloud. The database owner possesses a substantial amount of encrypted biometric data, which is stored in the cloud. When a user initiates an identification request, a query is sent to the database owner. The database owner generates a cipher text for the user's biometric trait and forwards it to the cloud for identification. The cloud server matches the encrypted query and returns the related index to the database owner. The database owner then computes the similarity between the query data and the associated biometric data identified by the index, subsequently providing the query result to the user.

The proposed work will focus on designing and implementing the biometric identification scheme. Key objectives include developing efficient encryption techniques to secure biometric data during transmission and storage in the cloud. Furthermore, privacy-preserving mechanisms will be devised to ensure that the biometric traits of users remain confidential. The research will also explore techniques to detect and resist collusion attacks that may arise between users and the cloud.

Overall, this project aims to contribute to the advancement of secure biometric identification in cloud computing, providing users with a privacy-preserving and reliable solution for personal identification. Through rigorous analysis the efficiency and effectiveness of the proposed scheme will be evaluated, paving the way for better biometric identification systems in the cloud.

Hardware Requirements:

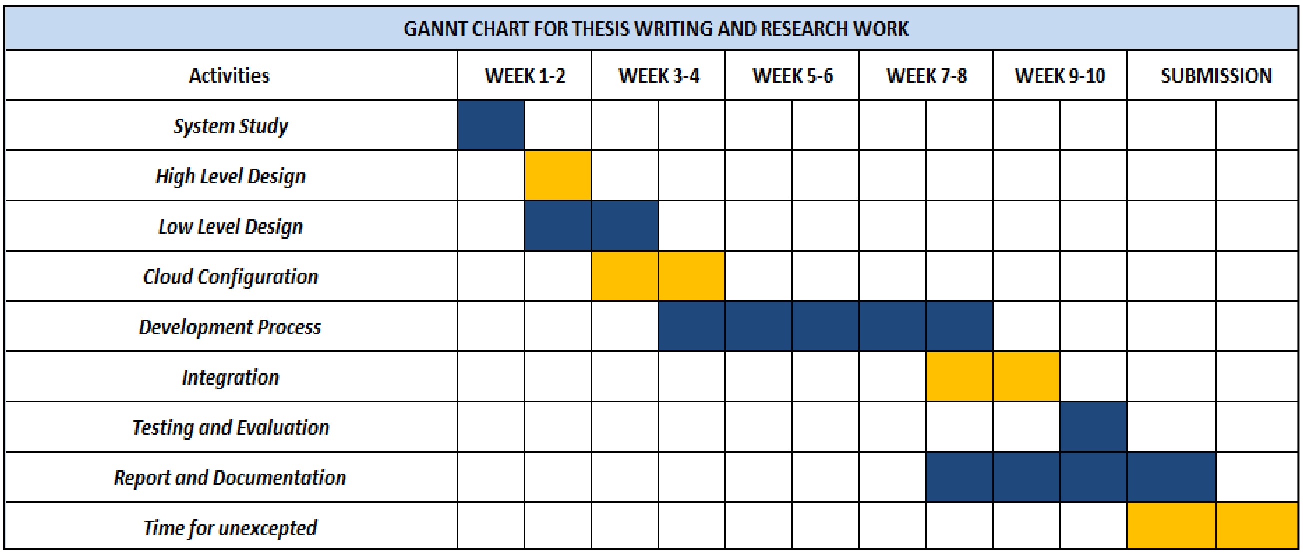
System	:	Pentium IV 2.4 GHz.
Hard Disk	:	500 GB.
Ram	:	4 GB

- *Any desktop / Laptop system with above configuration or higher level*

Software Requirements:

Operating system	:	Windows XP / 7
Coding Language	:	Java (Jdk 1.7)
Web Technology	:	Servlet, JSP
Web Server	:	Tomcat 6.0
IDE	:	Eclipse
Database	:	My-SQL 5.0
UGI for DB	:	SQLyog
JDBC Connection	:	Type 4 Driver

Plan of Work:



GANNT CHART FOR THESIS WRITING AND RESEARCH WORK												
Activities	WEEK 1-2		WEEK 3-4		WEEK 5-6		WEEK 7-8		WEEK 9-10		SUBMISSION	
System Study	🟦											
High Level Design		🟨										
Low Level Design		🟦	🟦									
Cloud Configuration			🟨	🟨								
Development Process				🟦	🟦	🟦	🟦	🟦				
Integration								🟨	🟨			
Testing and Evaluation										🟦		
Report and Documentation								🟦	🟦	🟦	🟦	
Time for unexcepted											🟨	🟨

Literature Survey:

1. Feature Level Fusion Using Hand and Face Biometrics

Multi biometric systems utilize the evidence presented by multiple biometric sources (e.g., face and fingerprint, multiple fingers of a user, multiple matchers, etc.) in order to determine or verify the identity of an individual. Information from multiple sources can be consolidated in several distinct levels, including the feature extraction level, match score level and decision level. While fusion at the match score and decision levels have been extensively studied in the literature, fusion at the feature level is a relatively understudied problem. In this paper we discuss fusion at the feature level in 3 different scenarios: (i) fusion of PCA and LDA coefficients of face; (ii) fusion of LDA coefficients corresponding to the R, G, B channels of a face image; (iii) fusion of face and hand modalities. Preliminary results are encouraging and help in highlighting the pros and cons of performing fusion at this level. The primary motivation of this work is to demonstrate the viability of such a fusion and to underscore the importance of pursuing further research in this direction.

2. Biometric-oriented Iris Identification Based on Mathematical Morphology

A new method for biometric identification of human irises is 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 endpoints 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) and the CASIA Iris Image Database (500 images). Compelling experimental results demonstrate the viability of using the proposed morphological approach for iris recognition when compared to a state-of-the-art algorithm that uses a global feature extraction approach.

3. Face Identification by fitting a 3D Morphable Model using Linear Shape and Texture Error Functions

This paper presents 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. Extensive identification results are available on our web page for future comparison with novel algorithms.

4. Efficient Privacy-Preserving Biometric Identification in Cloud Computing

Biometric identification is a reliable and convenient way of identifying individuals. The widespread adoption of biometric identification requires solid privacy protection against possible misuse, loss, or theft of biometric data. Existing techniques for privacy-preserving biometric identification primarily rely on conventional cryptographic primitives such as homomorphic encryption and oblivious transfer, which inevitably introduce tremendous cost to the system and are not applicable to practical large-scale applications. 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. Real experiments on Amazon cloud, over databases of different sizes, show that our computational/communication costs at the owner side are several magnitudes lower than the existing biometric identification schemes.

5. Filter bank-Based Fingerprint Matching

With identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometrics-based verification, especially fingerprint-based identification, is receiving a lot of attention. There are two major shortcomings of the traditional approaches to fingerprint representation. For a considerable fraction of population, the representations based on explicit detection of complete ridge structures in the fingerprint are difficult to extract automatically. The widely used minutiae-based representation does not utilize a significant component of the rich discriminatory information available in the fingerprints. Local ridge structures cannot be completely characterized by minutiae. Further, minutiae-based matching has difficulty in quickly matching two fingerprint images containing different number of unregistered minutiae points. The proposed filter-based algorithm uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length FingerCode. The fingerprint matching is based on the Euclidean distance between the two corresponding FingerCodes and hence is extremely fast. We are able to achieve a verification accuracy which is only marginally inferior to the best results of minutiae-based algorithms published in the open literature [6]. Our system performs better than a state-of-the-art minutiae-based system when the performance requirement of the application system does not demand a very low false acceptance rate. Finally, we show that the matching performance can be improved by combining the decisions of the matchers based on complementary (minutiae-based and filter-based) fingerprint information.

Literature References:

To work on research and implementation project, it is necessary to explore latest research and new development going on this field. In this project literature review is more inclined towards biometric cloud matching. The following references considered for literature review.

[1] X. Hei and X. Du, ''Biometric-based two-level secure access control for implantable medical devices during emergencies,'' in Proc. IEEE INFOCOM, Apr. 2011, pp. 346–350.

[2] 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.

[3] S. Romdhani, V. Blanz, and T. Vetter, ''Face identification by fitting a 3D morphable model using linear shape and texture error functions,'' in Proc. Eur. Conf. Comput. Vis., 2002, pp. 3–19.

[4] M. Barni et al., ''Privacy-preserving fingercode authentication,'' in Proc. 12th ACM Workshop Multimedia Secur., 2010, pp. 231–240.

[5] 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.

[6] A. Jain, L. Hong, and S. Pankanti, ''Biometric identification,'' Commun. ACM, vol. 43, no. 2, pp. 90–98, 2000.

Dissertation Outline Evaluation:

EC No.	Component	Excellent	Good	Fair	Poor
1.	Dissertation Outline	✓			

Particulars of the Supervisor and Examiner:

Items	Supervisor	Additional Examiner
Name	Krishna M G	Madanapalli Thousif Hussain
Qualification	Masters in Science (M.Sc.) Mathematics – Bangalore University	Masters in Technology (M. Tech) Computing Systems & Infrastructure – BITS PILANI
Designation	Quality Engineering Senior Manager	Cloud-operations Manager
Employing Organization and Location	Dassault Systemes, Bengaluru	Dassault Systemes, Bengaluru
Phone No.(with STD Code)	+91 -98860 24356	+91-8553079106
Email Address	krishna.g@3ds.com	mthousif.hussain@3ds.com

Remarks of the Supervisor:

The project chosen for dissertation is very much relevant to the scope of the industry current operation and working. This will help the student to enhance his knowledge in understanding of framework complexity and implementation details, the literature review included in the domain of research relevant and justified the level of dissertation for master studies. The outcome of this project helps the organization to take judicious decisions in cloud migration of biometric data together with implementation based on the requirement of the project and market needs.

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
WORK INTEGRATED LEARNING PROGRAMMES (WILP) DIVISION
SECOND SEMESTER OF ACADEMIC YEAR 2022-2023

SSZG628T: DISSERTATION OUTLINE

STUDENT ID No.	2021MT13176
NAME OF THE STUDENT	MANAM BHARADWAJ
STUDENT'S EMAIL ADDRESS	manam.bharadwaj@3ds.com
STUDENT'S EMPLOYING ORGANIZATION & LOCATION	Dassault Systemes, Bengaluru
SUPERVISOR'S NAME	Krishna M G
SUPERVISOR'S EMPLOYING ORGANIZATION & LOCATION	Dassault Systemes, Bengaluru
SUPERVISOR'S EMAIL ADDRESS	krishna.g@3ds.com
ADDITIONAL EXAMINAER'S NAME	Madanapalli Thousif Hussain
ADDITIONAL EXAMINER'S EMPLOYING ORGANIZATION & LOCATION	Dassault Systemes, Bengaluru
ADDITIONAL EXAMINER'S EMAIL ADDRESS	mthousif.hussain@3ds.com
DISSERTATION / PROJECT / PROJECT WORK TITLE	Efficient and Privacy Preserving Biometric Identification Scheme in Cloud Computing

Manam		
Signature of Student	**Signature of Supervisor**	**Signature of Additional Examiner**
Name: Manam Bharadwaj	**Name:** Krishna M G	**Name:** Madanapalli Thousif Hussain