National College of Ireland

Cloud Data Security through Hybrid Verification Technique Based on Cryptographic Hash Function

MSc Research Project
MSc Cloud Computing

Vinay Ranganath
Student ID: 20125119

School of Computing
National College of Ireland

Supervisor: Dr. Majid Latifi

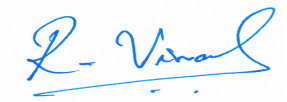
National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Vinay Ranganath
Student ID:	20125119
Programme:	MSc Cloud Computing **Year:** 2021 - 2022
Module:	MSc Research Project
Supervisor:	Dr. Majid Latifi
Submission Due Date:	16/12/2021
Project Title:	Cloud Data Security through Hybrid Verification Technique Based on Cryptographic Hash Function
Word Count:	**5028** **Page Count: 20**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 

Date: 16/12/2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Cloud Data Security through Hybrid Verification Technique Based on Cryptographic Hash Function

Vinay Ranganath
20125119

Abstract

Encrypted communications have a long history of use. Today, however, we can protect information confidentiality and privacy, which is critical to contemporary encryption research. Encrypted data is also used in research initiatives including human behaviour, financial transactions, and economic, political, and social events. In several areas of communication research, data security has taken centre stage. Everyone wants their data or information to be protected from theft or corruption. In this paper, we explore how to encrypt data in the cloud using a Hybrid Verification Technique based on Cryptographic Hash Function. We use Hybrid Verification Technique based on Biometrics and Encryption to increase cloud data security and 100 biometric picture samples were used in the experiment. Users are authenticated via biometric authentication, and subsequently their file storage data is secured using the AES algorithm. For strengthening the anonymity of cloud service provisioning, the TCHF-AED approach is described. Tiger is a cryptographic hash function that is used in TCHF-AED to provide a higher level of secrecy in cloud service provisioning. When storing data in the cloud, AES is more efficient than RSA encryption, according to the study.

1 Introduction

1.1 Background on the research topic

Nowadays cloud computing is widely used because of its easy access and high-level security and availability. Cloud computing is even more affordable for storing and accessing the information. Day to day use of cloud data is increasing because of access in two gatherings but its challenging to give security as well as privacy to increased users for cloud use (Kodada, 2021). In cloud computing data must be secure at all stages like while storing, while processing and also while uploading the data (Zaineldeen and Ate, 2020).

Research Problem

KP-ABE scheme was developed to generate the constant cipher text size in cloud. KP-ABE is performed with the help of Deler which is able to manage identity-based broadcast encryption system (Shen, Lu and Li, 2020). The KP-ABE scheme is essential to process the attribute-based encryption which supports senders to encrypt messages during the group of attributes and private key relationship with access structures. This aids to identify the decrypted cipher texts key holder. The access policy denotes monotone access structure in KP-ABE scheme. With the help of Diffie-Hellman exponent, the KP-ABE scheme provides

better security in selective-set method. However, time for encrypting the data and cost is improved in KP-ABE scheme (Shen, Lu and Li, 2020).

A Mediated Certificate Less Public Key Encryption (mCL-PKE) scheme was introduced to reduce the security difficulties in the cloud (Hwang and Le, 2018). The mCL-PKE scheme is applied to distribute the sensitive data from the public cloud in an efficient way. The secure storage and the key generation center are important in cloud. Based on available cloud users of public keys, the data holder encrypts the sensitive data in mCL-PKE scheme. After that with the aid of the access control strategy the encrypted data is transferred in the cloud environment. Then, the cloud decrypts the encrypted data through private keys for the users because of the complete authentication (Hwang and Le, 2018). This improves the security in Cloud Computing environment. But, due to the unauthorized access in cloud, the user provides the security and confidentiality issue in mCL-PKE scheme.

1.2 The Justification for the research

Cloud data security

Data Access Control, Data Authentication and Data Integrity. As a result, there is need for users that guarantee the data sent by a trusted sender and an unauthorized user does not initiate the false data acceptance. In order to address the data authenticity, a designed Message Authentication Code (MAC) is applied with the help of shared secret key.

Privacy Access Control

Group Key Management is a technique for safely allocating a message to a user group with confidentiality as the main key. Here users in a group have a symmetric key K, called the group key, and when to share a message, it must be encrypted with K and sent to the members of a group (Falohun, Fenwa and Oke, 2016). As K is known to all members of the group, they can decrypt and get the message. When the new user enters or exits a group, a new group key is created and distributed. No new member can get access to earlier transmitted messages (backward secrecy), and no user who has left the group can learn anything from future communications in the group (forward secrecy). This is the reason for rekeying when the user dynamics changes.

Privacy preservation of biometric template is done by non-invertible transforms. This transform creates a cancellable template which does not match with the original model. It is also impossible to reconstruct the original from a cancellable template. A new cancellable template is generated if the stored template is compromised, by changing distortion characteristics of the non-invertible transform (P and M, 2019). The aim of the irreversible transform is to eliminate minutiae correlation to the maximum possible extent.

Encryption In Cloud

Cloud Computing is the most emerging technologies in the world. Security is also very important in Cloud. Though there are no security issues in the cloud, still there is lack of security in the cloud. Attribute-based access control provides the flexibility of the method that supports data owners to combine data access policies within the encrypted data.

Encryption

In mCL-PKE scheme, the data owner encrypts the original text that depends on produced cloud user of public keys by using access control policy. Then, the encrypted data is

transmitted to the cloud environment. After that, the cloud decrypts the encrypted information for the users due to the efficient authentication. The mCL-PKE scheme achieves the encryption of data owner; and this improves the security level on the cloud environment (Hwang and Le, 2018).
The data hacking chance is more when our data is someone's server. So, to make more secure data and to make it more applicable we can use old biometric technique and encryption technique with combination. In proposed system we use fingerprint which is widely used for biometric and advanced encryption standard (AES) for security.

1.3 Main research questions

- How Hybrid Verification Technique based on Biometrics and Encryption system helps to address many cloud data security issues providing more reliable systems?

- What is the best solution to effectively improve Cloud Data Security and prevent unauthorized users and unintended access?

After this introduction, in Section 2, I describe the state-of-the-art works that are related to Cloud Security and applying Cryptography. In Section 3, I describe the methodology which has been used in the study. In Section 4, I describe the design specifications of the application and also discuss the implementation of the application and evaluation of the relevant results in section 5 and 6. Finally in section 7, I will also provide an overview of the future works which can be conducted based on the study.

1.4 Research Contribution

I propose another legitimate client validation for authentication and improve information security by a helpful hybrid system. This research incorporates both biometric check and encryption methodology in a solitary framework to guarantee legitimate client authentication. In the outcome the research will give a framework which guarantees the efficiency and security of the system.

2 Related Work

2.1 Introduction

Cloud services enable individuals to employ software and hardware controlled by third parties. Cloud Computing comprises provisioning and de-provisioning on demand and reduces the capital cost of software and hardware. Cloud provider hosts their services to the cloud storage by data owner. Security in cloud data storage is an essential one using cloud services provided by the service provider in cloud environment. The secured data

communication can be achieved through the confidentiality-based communication among cloud user and CSP.

Literature Survey:

According to (Merhav, 2019) “sensors offer raw image obtained from the person to be authenticated while signal processing algorithms do feature extraction from raw data while matching algorithms provide the match for the data thereby completing the decision process." In multi-modal systems, information fusion can be divided into many levels like feature-level, score-level, sensor-level, and decision-level. With different types of fusion, there is the difference in systems performance thereby creating a requirement to investigate the system based on biometric quality.

In (Haider, Rehman and Ali, 2020) methods of hybridizing cryptosystem and biometrics is presented. Methods of integrating face, fingerprint and palm print is proposed. Score Normalization in multimodal biometric systems used in their method.

Ranked Searchable Symmetric Encryption Scheme was developed by (Li, Zhou, Xu and Ge, 2020) for obtaining the efficient utilization of stored encrypted information in the cloud. OPSE mainly depends upon the exposed connection between the random order-preserving function. The order of plain texts was confined by executing encryption function. One-to-many order-preserving is applied for attaining significance score sharing in cloud.

In Generation of Biometric Key for Use in DES (Muttaqin and Rahmadoni, 2020), an image is given to model as input to produce 64-bitkey. The key is extracted from Thinned image using Binarization technique. The fingerprint can be further enhanced, and various other biometric features can be used to provide the most secure system. In an effective scheme for the generating cryptographic scheme is proposed.

(Shen, Lu and Li, 2020) presented a KP-ABE scheme for making the constant cipher text size. Based on the Delerablee identity-based broadcast encryption, KP-ABE scheme is performed. The trusted attribute authority in group has the potential to choose the three cyclic groups of prime order with the aid of bilinear pairing. The KP-ABE scheme accesses the private key by means of access structure. The encrypted cipher text is labeled according to the attributes set by performing decryption process and then receiver decryption key is associated with the LSSS scheme.

(Zhou, Zheng and Wang, 2020) followed an approach to safeguarding biometric data by template generation. Iris image characteristics are extracted, and iris template is generated then it is reduced to binary. The binary code is encrypted using AES cryptography. In receiving end, the templates are matched using template matching process (Muttaqin and Rahmadoni, 2020). If the match is found template is released, and it follows AES Decryption. The crypto key is generated using the iris template, which is stable throughout.

A secure data sharing scheme was introduced by (Ge et al., 2021) for achieving the key allocation and data sharing in cloud. It does not utilize the communication channel for key distribution process. With the aid of polynomial function, the secure data sharing scheme enhances the security of user revocation. The access control generally helps the group of secured user list that is signed through the group manager depending upon their signatures. Access control mechanism is used to guarantee the resources available to the authorized users and unavailable to revoked users and in the cloud environment.

2.2 Literature review matrix

Literature	Summary
(F.W.Olufade and J. Kolawole, 2012)	Biometric cryptosystem using face biometrics and Principal Component Analysis (PCA)
(Kwao, 2019)	Multiple cancelable identifiers from fingerprint images.
(Merhav, 2019)	Developed a valid biometric authentication system
(Merhav, 2019)	The key generation with binary biometric templates. Iris biometric combined with cryptographic applications securely
(Muttaqin and Rahmadoni, 2020)	digital signatures and cryptography key generation with biometrics.
(Zhou, Zheng and Wang, 2020)	Created a structure to generate stable cryptographic keys from biometric data.

Table 1: Overview of the Existing Biometrics-based authentication systems

3 Research Methodology

3.1 Proposed Work

TCHF-AED technique is presented for increasing the confidentiality of cloud service provisioning. Tiger is also known as cryptographic hash function which is employed in TCHF-AED to attain greater confidentiality rate in cloud service provisioning. At first, users transmit the attribute cloud request to the CSP (Hossain and Al Hasan, 2020).

3.2 Proposed Methodological Approach

Proposed hybrid architecture of biometric and encryption system

In proposed work I have used Fingerprint scanner to scan users finger image and then that scanner will return finger minutiae data and this minutiae data will be stored at cloud but we don't have any scanner so I am using below finger minutiae images and these images are saved inside 'Sample BiometricImages' folder.

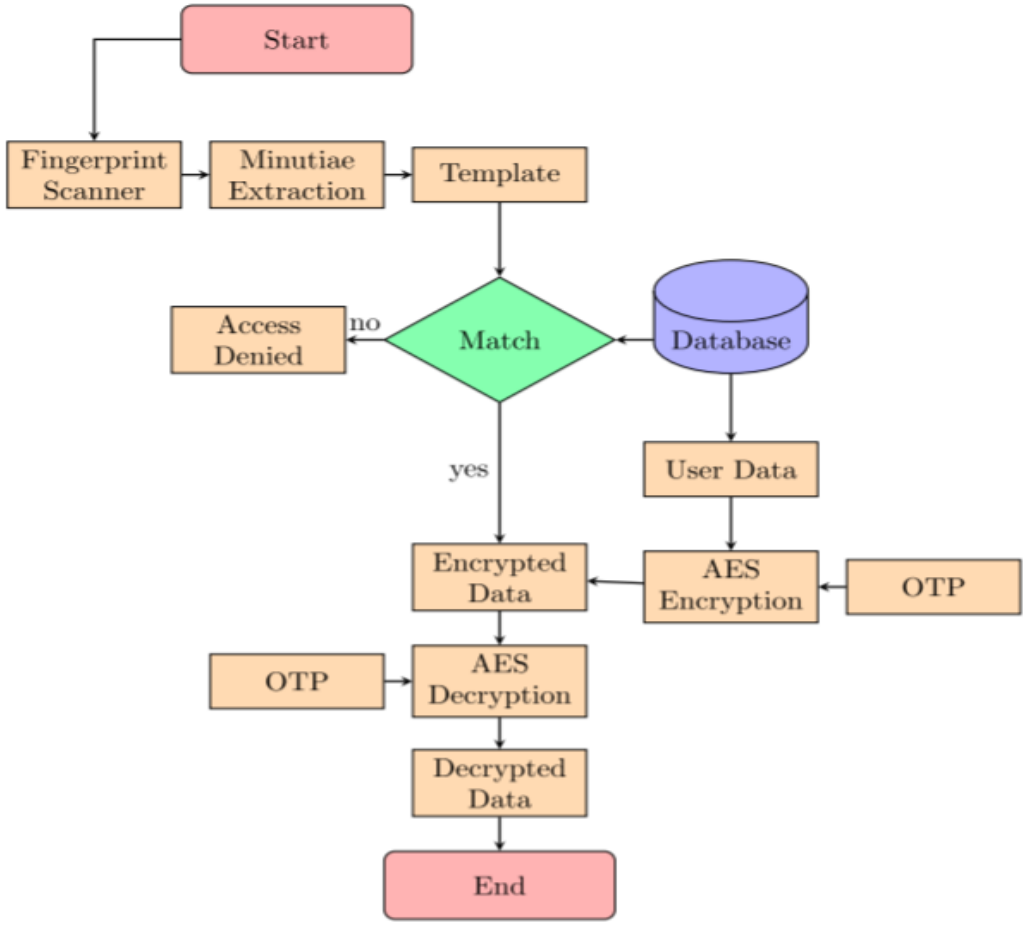


Figure 1: Block Diagram of Proposed System (Hossain and Al Hasan, 2020)

Generation of Secure Biometric Keys

The encryption key is now used for encrypting the passwords using AES encryption/decryption process. If needed dual encryption/decryption can do as two ciphers are generated thereby increasing the security level. Figure 1 shows the proposed methodology for generation of secure biometric keys for encryption/decryption process.

Above figure shows block diagram of proposed system and below we mentioned algorithm steps in detail as,

Algorithm 1 Procedure hybrid verification architecture through biometrics and encryption system

1: Collect biometric sample from user in client side.
2: Extract feature from biometric sample as template using minutiae extraction algorithm.
3: Verify the template using store template in cloud database. If success goto step 4 else access denied.
4: Send login request to the server.
5: Cloud authentication server randomly generate a OTP from unique characters. Then encrypt user data using the AES encryption algorithm and send the encrypted data to the client side.

$$ED \rightarrow AESEncrypt(Data, OTP)$$

6: Cloud authentication server also send the OTP to the user using the http gateway.
7: User decrypt the encrypted data using the OTP.

$$Data \rightarrow AESDecrypt(ED, OTP)$$

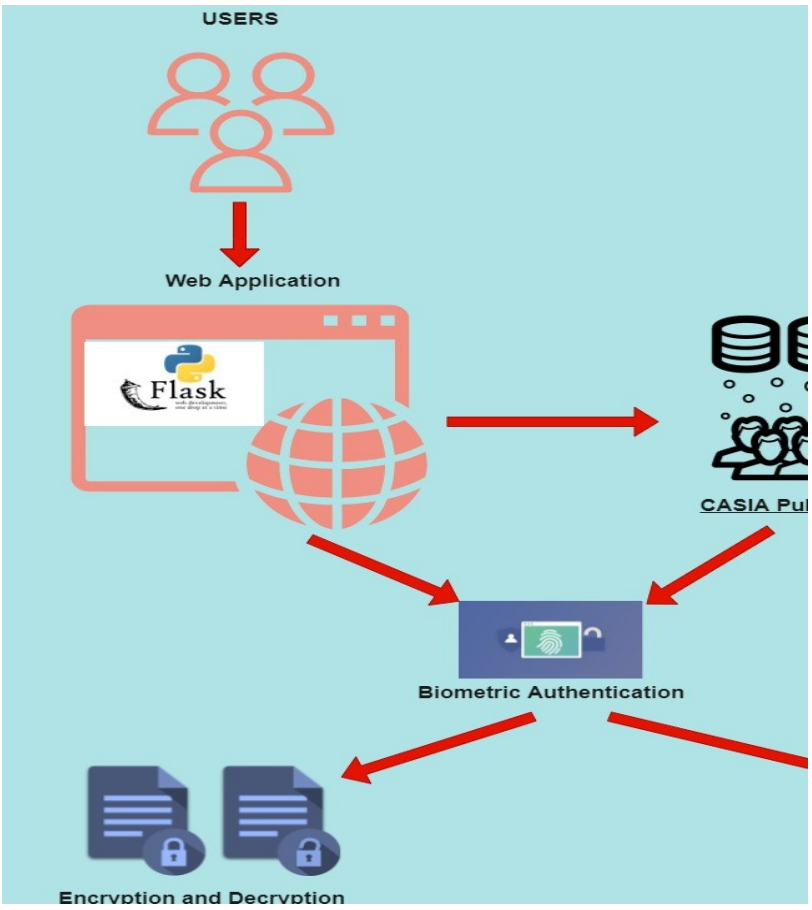


Figure 2: Architecture Diagram

3.3 Justifies the choice of methods

Encryption Methods in Cloud

A new model was designed by (Hossain and Al Hasan, 2020) for adaptive encryption of public cloud databases between the data confidentiality of cloud database structures. An original cost model was used for assessing cloud database services for encrypted instances. The model considered the variance of cloud prices and tenant workloads in medium-term period. Though the data confidentiality was improved, the storage overhead remained unaddressed.

mCL-PKE scheme was designed by (Hwang and Le, 2018) without any pairing operations. mCL-PKE scheme built the practical solution for distributing sensitive data issues in public clouds. The cloud was used as secure storage and key generation center. The data owner encrypted data by user's public key with access control policies and uploaded data.

A new encrypting algorithm was designed by (Rachmawati, Andri Budiman and Aulia, 2018) depending on symmetric key cryptography. Logical operations are such as XOR and zero padding. Encryption algorithm created the key using the Monoalphabetic secret sharing algorithm. This algorithm provides an efficient secure communication in Cloud.

4 Design Specification

The biometrics (fingerprint) is obtained from **CASIA database,** and 10 samples are taken (BIT, 2021).

Biometric Key Generation

First, the core point of minutiae from the fingerprint is extracted from the fingerprint image. The availability of inexpensive and compact solid-state scanners as well as important fingerprint matches are two important reasons for fingerprint-based identification methods (M.K and K.R, 2021).

Xor1 operation is done for the binary of fingerprint value and iris value which is XORed again with binarized palmprint feature to get xor2. The biometric keys are later compressed to Hexadecimal value which can act as an encryption key.

Properties, Vulnerabilities and Performance Measurements of Biometrics

Biometric Properties

The following properties of biometric must be maintained for proper biometric comparison with previously stored characteristic:

a) Invariance: The property of biometric being constant over long period of time.
b) Measurability and Timeliness: The property of biometric template of being measured in less time.
c) Singularity: The property of biometric being unique.
d) Reducibility: The property of biometric of being reduced so that easy storage is possible.
e) Reliability: The biometric should be reliable and privacy of a person should not be disturbed.

Techniques

The new cryptosystems technique aggregated any secret keys and created as single key with the power of all collected keys. The aggregate keys were secretly sent and maintained in smart card with minimal storage space consumption.

Existing Techniques and Drawbacks

There are many existing techniques for cloud computing security and even need of more advanced technique for improving security level. Cloud computing is used in many fields because of many recent innovations in it as well as it can be accessible without any other software installation. Cloud information security can use biometric with multimodality. Unimodality used for cloud security has many problems such as inappropriate information, less security applicable. Previous authors even used facial features for security but while verification it may have crossover problems. Many previous researchers uses asymmetric key and cryptography for encryption which is old compare to new encryption techniques like AES.

So, to avoid the existing technique problems we designed proposed integrated technique by fingerprint biometric and AES advanced encryption security.

Merits and Demerits of Biometric Techniques

None of the biometric technique is 100% secure, but when it is related with knowledge-based techniques like PIN or a password, biometrics are highly secure. The merits and demerits of biometric techniques is short in table 2.

Table 2 General Merits and Demerits of Biometrics

Advantages	Disadvantages
Positive identification	Public acceptance
Biometrics will not be lost or forgotten	Legal issues
Biometric templates are unique for each Individual	Hardware cost increases
Rapid identification authentication	Huge storage required
Costs in general are decreasing	Privacy concern

5 Implementation

Implemented solution

The proposed technique utilizes the MQTT IOT simulator in the cloud environment.

Step 1 Biometrics Sensing

- This step helps to recognize the biometric information of the users via sensors. The information of human biometrics Fingerprint, Palm print and Iris are collected.

Step 2: Pre-processing -Feature Extraction

- After pre-processing, the required features from each biometric are extracted in form of decimals which are then used to convert binary value.

Step 3: Normalization and Fusion

- After normalizing, the features are fused by following the xor operation of the biometric values obtained.

Step 4: Generation of Keys

- Using binarized biometric features, keys are generated.
- The two binary keys generated are used for providing 2 levels of security.

Step5: Encryption and Decryption Description

- The module follows the process of encryption and decryption by incorporating AES encryption process.

The above process is reversed during authentication. The proposed algorithm that uses cancellable template is secure against many attacks.

In proposed work, I use Fingerprint scanner to scan users finger image and then that scanner will return finger minutiae data and this minutiae data will be stored at cloud but we don't have any scanner, so I am using below finger minutiae images and these images are saved inside 'SampleBiometricImages' folder.

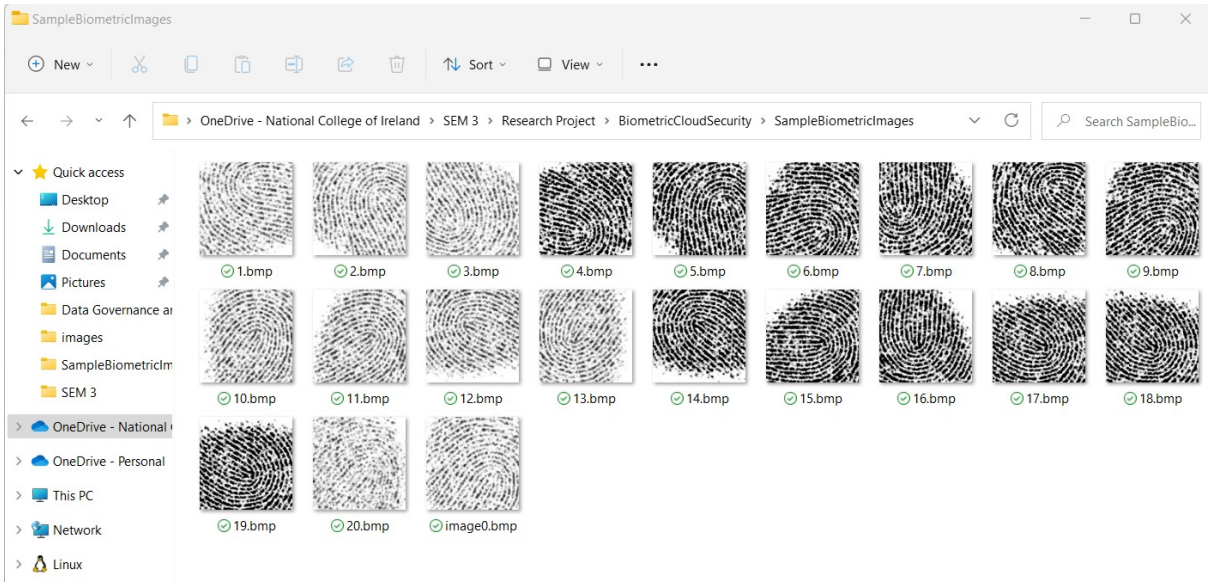


Figure 3: Sample Biometric Images taken from CASIA

From above screen you can use any image to signup user with cloud application

To implement this project, we have designed following modules

1) File Upload: using this module user can upload file and this file will be encrypted using AES algorithm and OTP key and then file stored at cloud server
2) Download File: user can select any desire file and then cloud server will accept selected file and then decrypt that file using users OTP key and then send that file back to user for download.

6 Evaluation

The implementation of the proposed framework with fingerprint biometrics is evaluated with the CASIA biometric template database which is a repository of many biometrics like iris, palmprint and face images. During registration phase, a user provides three biometric samples to the system. Two samples are used to generate the key, and another (belonging to different modality) is used to authenticate the user. In the enrollment phase the following steps are performed:

a) Sensor acquires the biometric data

b) Data is preprocessed from which features are extracted. Cryptographic key is generated from the biometric template after fusing the two biometrics.

c) The hash of the cryptographic key is calculated.

d) Another sensor gets the biometric data used for authentication

e) This unimodal template is processed, and cancelable biometric fingerprint template is generated with non-invertible transforms.

f) The hash of key generated and cancelable biometric template is stored in look-up table.

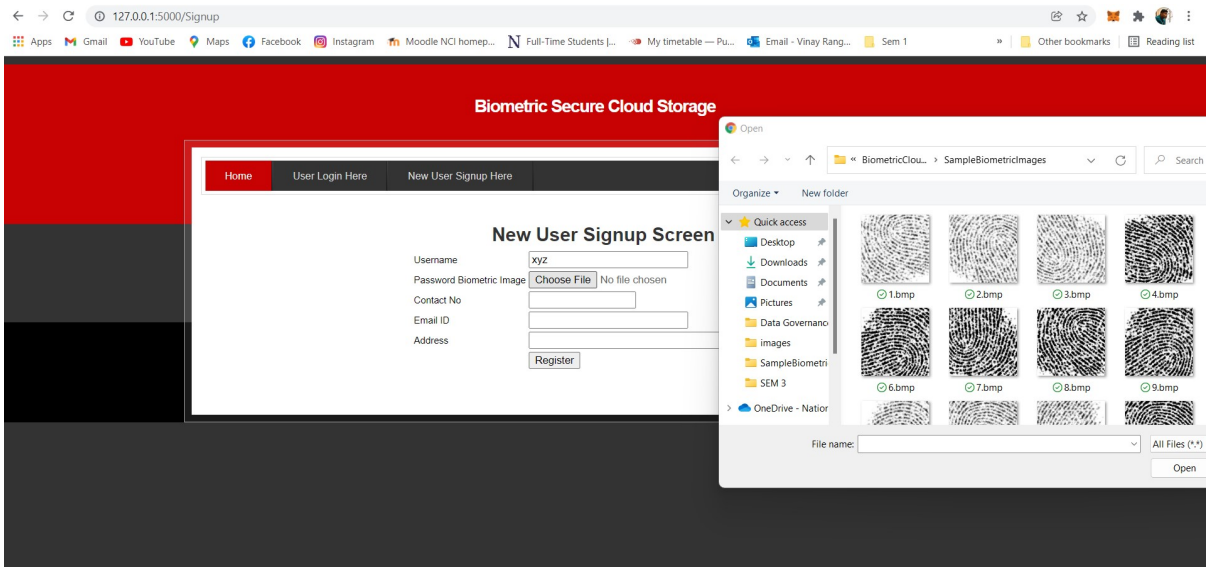


Figure 4: Registration Phase

During the verification phase, a user first provides three biometric samples which are converted to cryptography key. The generated keys hash and cancellable biometric template are produced from biometric samples. If the hash does not match with the one found in a lookup table, the key is not released, and the user must provide his biometric sample again. If hash that is matching is found, a similarity score is calculated between the generated cancellable biometric template and the one present in look-up table matching to the hash. From this procedure, the person is authenticated.

Authentication is provided only if:

a) Hash produced from the key during registration is found in look-up table.

b) Similarity score found between the generated cancelable fingerprint template, and one present in the look-up table is within threshold limit which is predefined.

Frameworks Security Level Evaluation

The proposed system stores only the hashes of generated keys (obtained by fusion of two unimodal keys) in the look-up table. Small variation can result in different keys and hence different hash. Authentication happens only if proper hash is found and hence the system produces robust, stable key.

False acceptance is less in the system as biometric templates privacy is protected by one-way hash functions and non-invertible transforms. Even if the hacker obtains access to the look-up table, it is impossible for him to regenerate the key/ biometric templates created during enrolment phase.

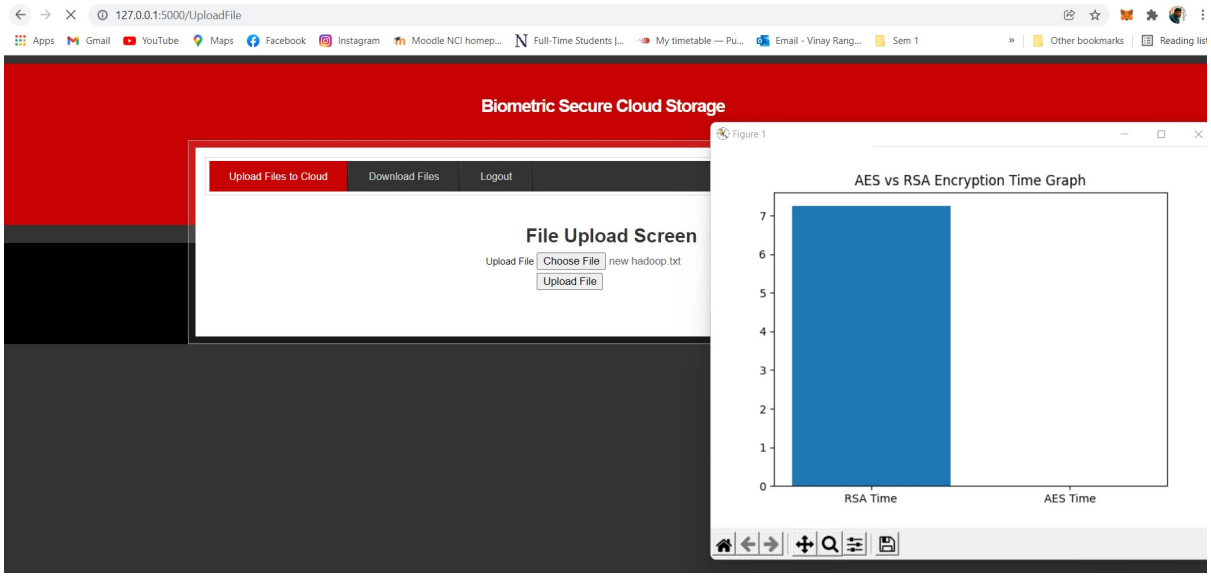


Figure 5: Encryption Time Graph

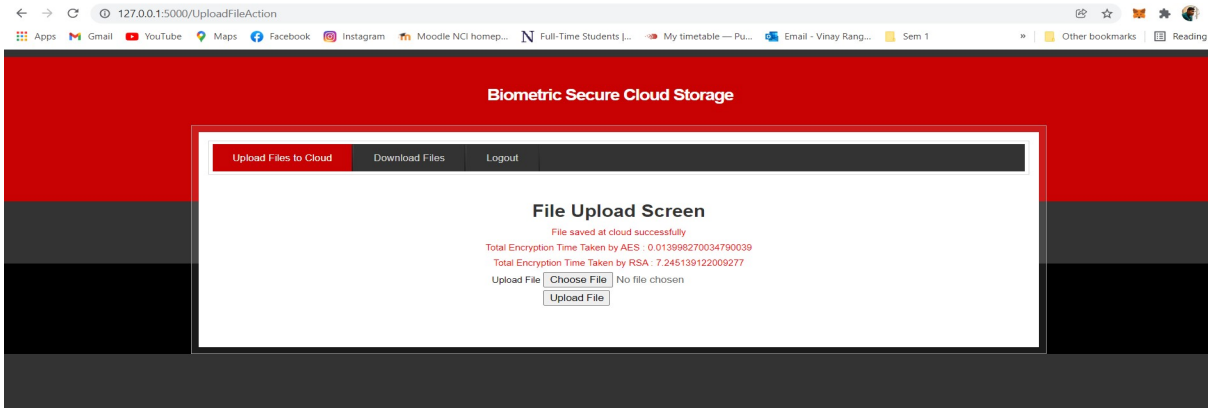


Figure 6: Encryption Time Taken

6.1 Experiment / Case Study 1

We will upload data to the cloud and login securely using biometrics for the sake of testing the program. The uploaded file is tested to see whether it's been encrypted properly after it's been uploaded to the cloud.

In Case Study 1, the source file to upload to the cloud storage application is a text document (.txt file), and the uploaded file is examined. The file is then decrypted, and the success of the decryption is checked.

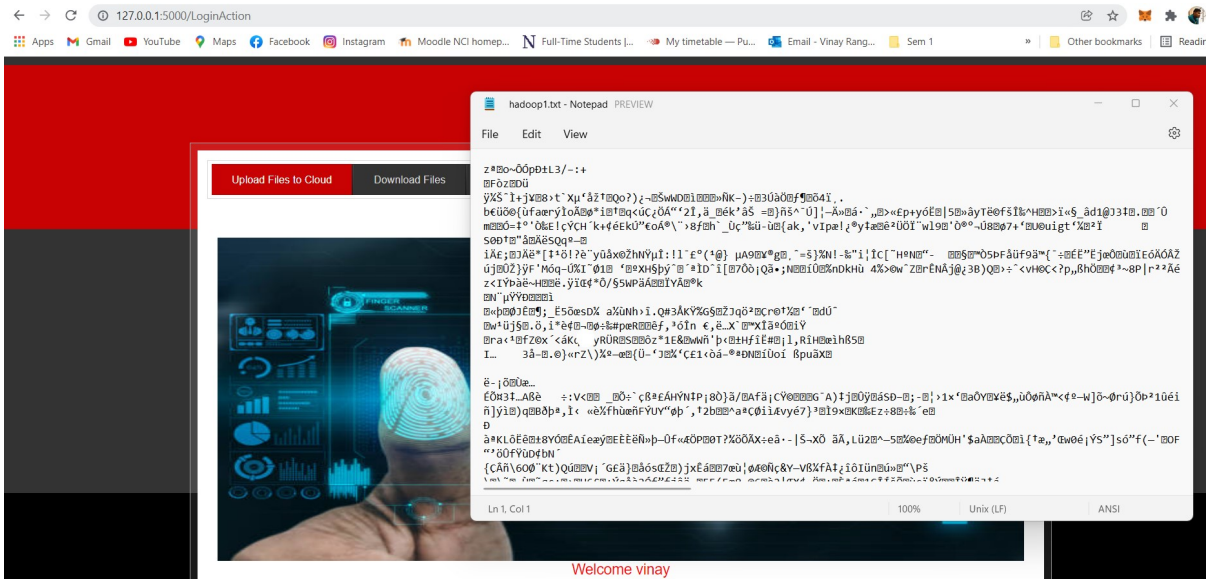


Figure 7: Encrypted Text Document

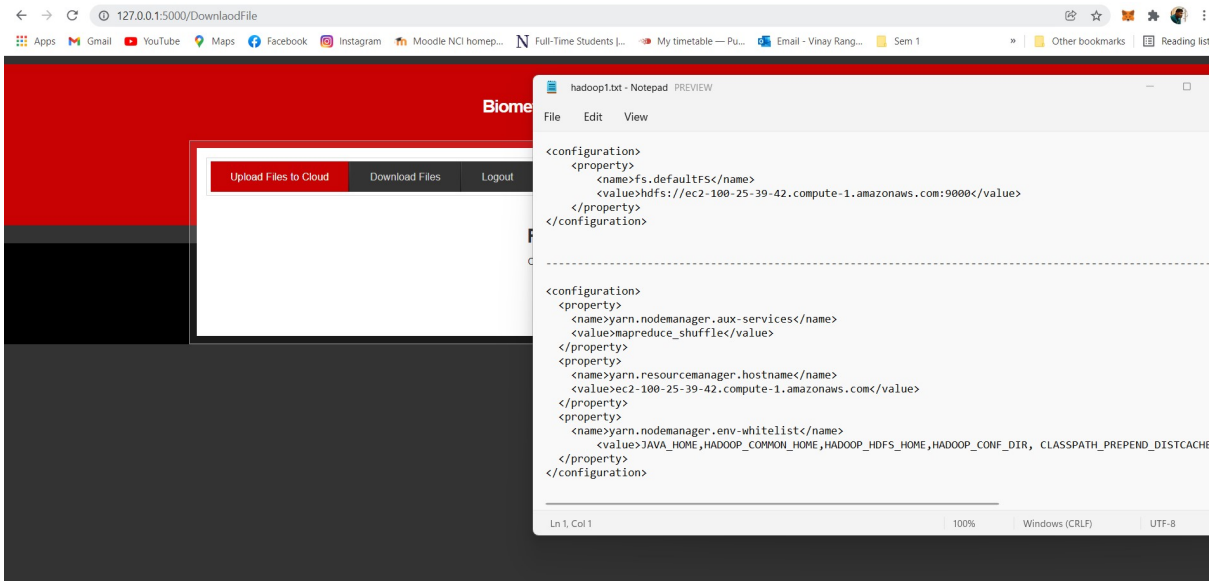


Figure 8: Decrypted Text Document

6.2 Experiment / Case Study 2

In case study 2, I will be trying to access the cloud storage application using the incorrect biometric image. When the incorrect biometric picture is used to log into the program, a template mismatch occurs, resulting in an error message being shown. This makes the program more secure, as logging in without the necessary biometrics is impossible. I'll try to upload a photo (.jpg) file and see if the encryption and decryption operations are successful.

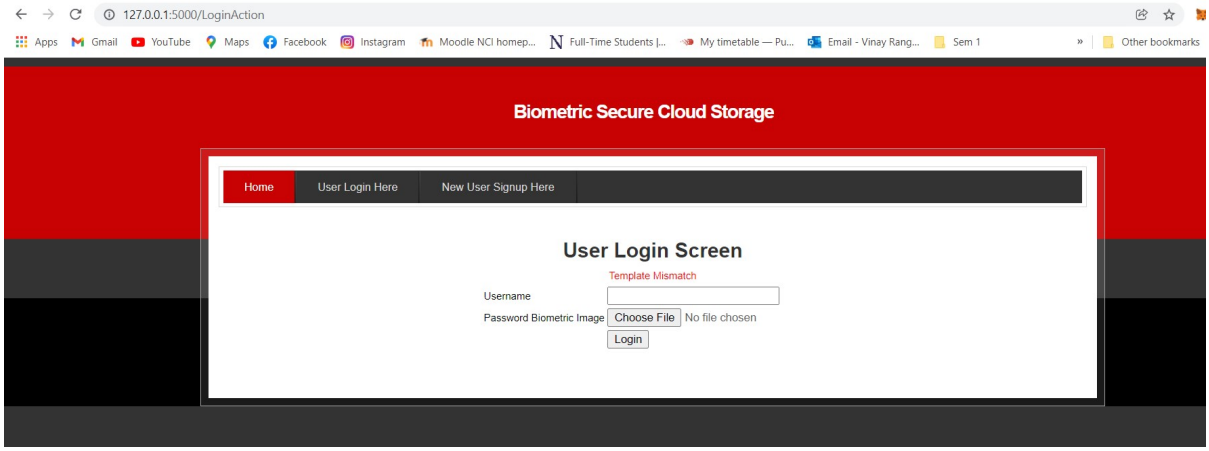


Figure 9: Template mismatch if Incorrect Biometric Image is Chosen

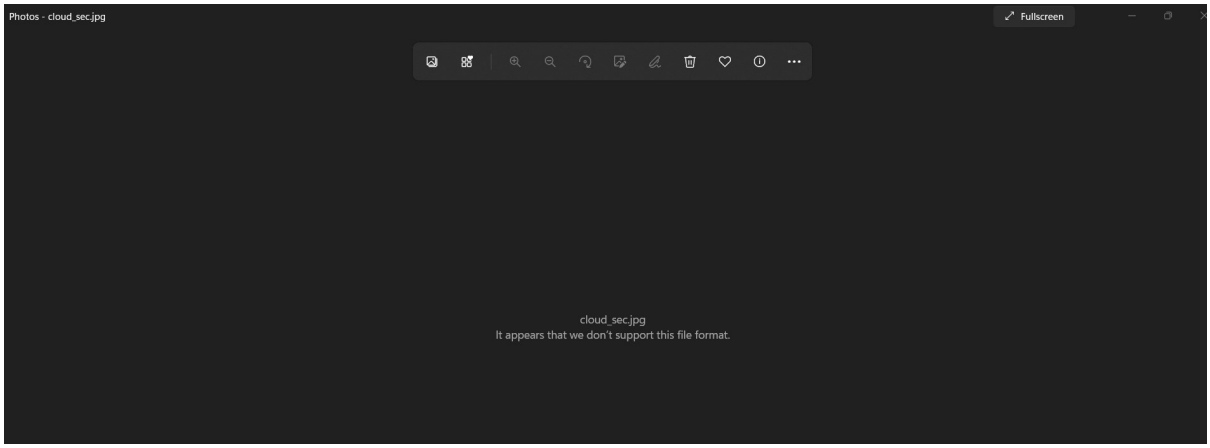


Figure 10: Encrypted .jpg File

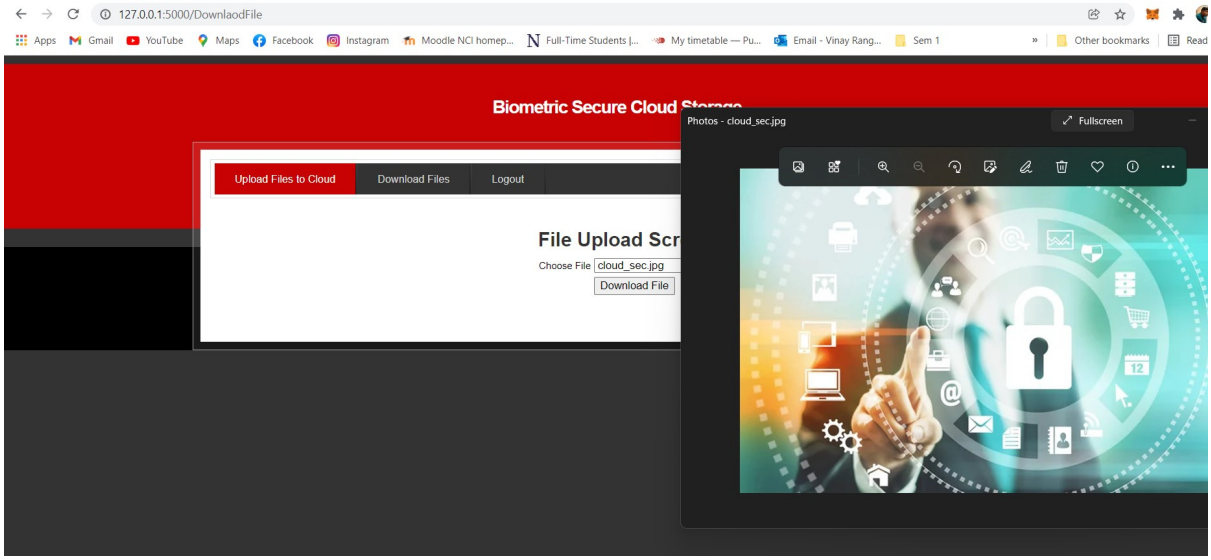


Figure 11: Decrypted .jpg File

6.3 Discussion

Encryption In Cloud

An efficient multi-user searchable attribute-based encryption scheme was developed by (Lin and Jiang, 2020) with attribute revocation for cloud storage. The keyword searchable function was attained, and security of scheme was minimized to Bilinear Diffie-Hellman (BDH) assumption. The designed scheme was more secure under Indistinguishability against discriminating Ciphertext-Policy and Plaintext Attack (IND-sCP-CPA). But the memory consumption was not minimized using efficient multi-user searchable attribute-based encryption scheme.

But CP-ABE schemes failed to directly use in cloud storage system. An effective and secure access control scheme was introduced by (Zhou, Zheng and Wang, 2020) for shared data to address the security problem. The designed scheme enhanced the security level of CP-ABE based scheme. However, the encryption time was not minimized using secure access control scheme.

Data encryption, homomorphic encryption and secret sharing algorithms were employed by Muhil et al. (2015) for secured data outsourcing. The essential problem with data storage was CIA (Confidentiality, Integrity, and Availability). The single cloud underwent the security issues which were obtained for multi-cloud called cloud of clouds or interclouds (Nicholas, Wilson and Muthoni, 2018).

In this project we are providing hybrid biometric verification which will secure user biometric data with encryption algorithm and then user will get authenticate with his biometric data. In existing system all user’s biometric data will be stored in plain format at cloud server and if malicious users hack cloud, then entire biometric data will be exposed to malicious users and then he can make clone of biometric data to bypass authentication system.

To overcome from above issue, we are applying hybrid technique which will allow user to authenticate himself with his biometric data and then this biometric data will be encrypted and stored at cloud server, if malicious user hack this data then he can’t make clone out of encrypted data.

Now-a-days in market lots of encryption techniques are available and to choose best one with less computation cost we have compared performance of AES and RSA in Python environment.

7 Conclusion and Future Work

Python was used to successfully design the proposed system. It secures numerous programs by employing fingerprint authentication to authenticate users and then using the AES method to encrypt users' file storage data. Python MQTT IOT is the simulator utilized in this suggested system. In the subject of how a hybrid verification technique based on biometrics and an encryption system aids in the resolution of various cloud data security challenges. By

analysing the results, we can show that the suggested system is more secure than existing state-of-the-art solutions. Users were authenticated using biometric authentication, and subsequently their file storage data was secured using the AES algorithm.
All files uploaded by users will be encrypted using the OTP secret key, and only when the user authenticates with a valid Biometric image will the OTP be triggered, allowing the user to decrypt data stored in the cloud. We will deploy our application on public cloud platforms such as AWS and Azure as part of our future effort, adding an extra degree of security. To evaluate the outcomes of the proposed cloud security solution, I'll also be adding more python libraries. I'll also think about constructing the cloud environment in cloud environments like AWS, Azure, or Google Cloud Platform. The authentication will be enhanced by implementing a two-factor authentication system based on OTP and integrating it with cloud platforms. I'll examine the performance of RSA and AES encryption in ensuring cloud data security, as well as incorporating biometrics into the cloud so that data has an extra layer of protection in cloud storage security.
The main contributions of the work are abridged as follows:

(a) Biometric comprising of the fingerprint with efficient fusion and a stable key mechanism is proposed.
(b) A secure framework that provides biometric template privacy and 0% false acceptance rate is proposed.
(c) Multifactor authentication for data access in a cloud is proposed.
(d) Secure technique for file upload and download from a cloud is recommended.

References

Biometrics.idealtest.org. (2021). *BIT*. [online] Available at: http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Fingerprint [Accessed 16 Dec. 2021].

Falohun, A., Fenwa, O. and Oke, A., 2016. *An Access Control System using Bimodal Biometrics*. International Journal of Applied Information Systems, 10(5), pp.41-47.

Ge, C., Susilo, W., Baek, J., Liu, Z., Xia, J. and Fang, L., 2021. *A Verifiable and Fair Attribute-based Proxy Re-encryption Scheme for Data Sharing in Clouds*. IEEE Transactions on Dependable and Secure Computing, pp.1-1.

Haider, S., Rehman, Y. and Ali, S., 2020. *Enhanced Multimodal Biometric Recognition Based upon Intrinsic Hand Biometrics*. Electronics, 9(11), p.1916.

Hossain, M. and Al Hasan, M., 2020. *Improving cloud data security through hybrid verification technique based on biometrics and encryption system*. International Journal of Computers and Applications, pp.1-10.

Hwang, S. and Le, M., 2018. *Efficient certificate-based encryption and hierarchical certificate-based encryption schemes in the standard model*. Journal of Intelligent & Fuzzy Systems, 35(6), pp.5971-5981.

Kodada, B., 2021. *Data Security Challenges in Cloud Computing. Academia Letters*,.

Kwao, L., 2019. *User Authentication Model for Securing E-Health System using Fingerprint Biometrics*. International Journal for Research in Applied Science and Engineering Technology, 7(11), pp.285-293.

Li, Y., Zhou, F., Xu, Z. and Ge, Y., 2020. *An Efficient Two-Server Ranked Dynamic Searchable Encryption Scheme*. IEEE Access, 8, pp.86328-86344.

Lin, H. and Jiang, Y., 2020. *A Multi-User Ciphertext Policy Attribute-Based Encryption Scheme with Keyword Search for Medical Cloud System*. Applied Sciences, 11(1), p.63.

M.K, N. and K.R, R., 2021. *Secured Key Generation for Biometric Encryption using Hyper-chaotic Map and DNA Sequences*.

Merhav, N., 2019. *Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation*. IEEE Transactions on Information Theory, 65(4), pp.2477-2491.

Muttaqin, K. and Rahmadoni, J., 2020. *Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based*. Journal of Applied Engineering and Technological Science (JAETS), 1(2), pp.113-123.

Nicholas, K., Wilson, C. and Muthoni, A., 2018. *Enhancing Confidentiality and Integrity in Cloud Computing using RSA Encryption Standard and MD5 Hashing Algorithm*. International Journal of Computer Applications, 181(14), pp.23-27.

P, J. and M, A., 2019. *Secure Data Access Control and Privacy Preserving Techniques in Private Cloud Environment Using Secure Un-Crackable Dynamic Double Encryption Standard*. Journal of Advanced Research in Dynamical and Control Systems, 11(11-SPECIAL ISSUE), pp.746-760.

Rachmawati, D., Andri Budiman, M. and Aulia, I., 2018. *Super-Encryption Implementation Using Monoalphabetic Algorithm and XOR Algorithm for Data Security*. Journal of Physics: Conference Series, 979, p.012033.

Shen, C., Lu, Y. and Li, J., 2020. *Expressive Public-Key Encryption With Keyword Search: Generic Construction From KP-ABE and an Efficient Scheme Over Prime-Order Groups*. IEEE Access, 8, pp.93-103.

Zaineldeen, S. and Ate, A., 2020. *Improved cloud data transfer security using hybrid encryption algorithm*. Indonesian Journal of Electrical Engineering and Computer Science, 20(1), p.521.

Zhou, Y., Zheng, S. and Wang, L., 2020. *Privacy-Preserving and Efficient Public Key Encryption with Keyword Search Based on CP-ABE in Cloud*. Cryptography, 4(4), p.28.