Cloud Data security enhancements through the biometric and encryption system

MSc Research Project
MSc Cloud Computing

7

Preetham Babu Dinesh Babu
Student ID: 21156514

School of Computing
National College of Ireland

Supervisor: Punit Gupta

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Preetham Babu Dinesh Babu		
Student ID:	21156514		
Programme:	MSc Cloud Computing	**Year:**	2022-2023
Module:	MSc Research Project		
Supervisor:	Punit Gupta		
Submission Due Date:	15/12/2022		
Project Title:	Cloud Data Security Enhancements through the Biometric and Encryption System		
Word Count:	8263	**Page Count -**	25

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: Preetham

Date: 15/12/2022

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:	

Table of Contents

Cloud Data Security Enhancements through the Biometric and Encryption System

Preetham Babu Dinesh Babu
Student ID - 21156514

1 Abstract

Data and information security are one of the key issues that is persistent with growing technology. Data Security becomes the biggest challenge since more and more data are being shared and stored across network and the data can be stolen, modified, deleted or accessed by illegitimate users. Hence there is a need to secure sensitive data in such a way to alleviate threats relating to security and privacy of data. Security acts as a key challenging factor for safe storage of data. The proposed research work puts forward the idea of security architecture using biometric authentication mechanism and encryption with significant contribution to biometric image pre-processing, feature extraction and encryption algorithm. In this thesis research report we are going to work on the Cloud Data security and methods to enhance the cloud data security through the biometric and encryption authentication system where user can sign up with biometric data and after correct login they can upload any file and all files will be uploaded to Amazon AWS account in encrypted format and biometric data will also be saved in AWS S3 bucket in encrypted format. Researcher experimented with 3 different encryption algorithms such as AES, RSA and ECC and their performance was evaluated in terms of computation time. The results obtained will show us the best possible encryption system that can be used.

Keywords: RSA (Rivest-Shamir-Adleman) algorithm, Elliptic Curve Cryptography (ECC)algorithm, Advanced Encryption Standard (AES)algorithm, Cloud Computing, Cloud Data security, biometric and encryption system.

2 Introduction

2.1 Background Of Study

In this research, “background work” we analysed and proposed for the enhancements through the biometric and encryption authentication system. In this thesis research report researcher to build Cloud Data security enhancements through the biometric and encryption authentication system where user can sign up with biometric data and after correct login they can upload any file and all files will be uploaded to Amazon in encrypted format and biometric data will also be saved in Amazon in encrypted format. Researcher experimented with 3 different encryption algorithms such as AES, RSA and ECC and their performance was evaluated in terms of computation time.

2.1.1 Cloud Data Security:

Cloud security is highly essential especially when storage is offered as a service by CSPs **(khandelwal & Chauhan, 2021).** End users store their sensitive data on cloud and due to the virtual nature of cloud, users do not know where the data is actually stored. Hence robust security controls will enable the CSPs to reassure that the users sensitive data are safe. With new security controls introduced, hackers find new ways of breaking security walls. There are a number of security measures that are currently implemented in cloud environment to ensure safe transaction in cloud. These include data integrity checks for ensuring that the stored data is unchanged, data replication for recovery, access control mechanisms, encryption mechanisms for data protection etc. **(Zhao & Xu, 2022).**

2.1.2 Biometric:

Biometrics refer to body measurements and statistical analysis of human's physiological and behavioural traits **(Uhl & Rathgeb, 2021)**. No two persons have the same biometric traits, thus make it highly unique among individuals. Due to its discriminative nature, biometrics are used in identification, duplicate checking and verification of individuals which can be applied to authentication system, forensic investigations, access control and fraud detection **(El- El-Sofany, 2022**).

There are variety of physiological traits in human body ranging from commonly used fingerprints, finger vein etc. to rarely used traits like tongue, ear, retinal scans etc. Behavioural traits include signature, gait, speech and keystroke dynamics.

The proposed research work uses fingerprint biometric traits for security enhancement. The below section briefly discusses trait.

This is mainly due to that the acquisition process of the biometric feature is minimally invasive. Biometrics is the measurement of biological data **(Nishiuchi & Soya, 2011)**, the term is commonly used to refer to the recognition of a person by physical characteristics such as fingerprint or behavior characteristics as signature and the way they walk. Today biometrics has a great scope in criminal, government, and commercial systems **(Smith et al., 2018)**, gaining wide acceptance as one of the most effective technologies for people authentication in a wide range of informatics applications.

The implementation of biometric and encryption system in Cloud as a means of security through public or private networks, has generated more concern for the security of the biometric data. Analysis made by several authors **(Amedzro St-Hilaire, 2020)** detected eight points of vulnerability in the overall architecture of a biometric system in which it is possible to obtain the biometric trait.

The vulnerability points in the general architecture of an automatic fingerprint identification, which are of interest for this research are those by which it is possible to obtain the minutiae template partially or completely. These are:
1) The of biometric features extractor.
2) The communication channel between the extractor and the biometrics comparator.
3) The comparator of biometric features.
4) The communication channel between the comparator and the biometrics features database.
5) The biometric database.

2.2 Encryption:

Encryption is a standard and conventional way of securing data and information. It is a technique in which plain text is converted into a different form and stored in a form such that anyone who tries to read the data/information cannot do so. This is because the encrypted file does not convey the original meaning.

2.3 Research problem

With cloud computing growing at a faster pace, threats relating to the associated data also increases. Data storage in cloud environment is highly vulnerable to theft and leakage. There are various instances of data theft, breaking of security walls by hackers despite restricting the access by authentication based on passwords and tokens. Such modes of authentication tend to be weak. In addition to such weaknesses, there exists a lack of strong interconnection between the users and their data.

In order to address these limitations, there is a need for a comprehensive security solution which provides a strong authentication mechanism as well as a highly secured data protection system, thus providing a secured environment to end users.

2.4 Research Question

1. Why is the verification process required to access the data in the cloud when there is massive computation power or load in the cloud network?
2. How the Data will be secured through the integration of biometric and encryption system compared to the normal authentication process when there are security threats that should be averted to reassure the users?

2.5 Objective

To provide more reliable cloud data security enhancements through Biometrics and encryption system. To develop a model which enables the cloud user to store the data in an encrypted manner and will be utilizing biometrics for accessing the data.

3 Literature Review

3.1 Introduction

This chapter outlined the various research works in the areas of security architectures in cloud computing environment, various biometric and encryption systems, Cloud Data security enhancements techniques, feature extraction techniques and varied encryption mechanisms.

3.1.1 Important Security issues in the Cloud

(Wichmann et al., 2021) Brute Force Attacks type of attack consists in guessing a finite set of identification characteristics, the sufficient amount to identify a person. Usually, the difficulty of performing a brute force attack is expressed in number of operations necessary for successfully reconstructing the biometric template. To perform this attack, a randomly generated template is sent and the satisfaction criteria is evaluated. This criterion consists in checking how many elements of the generated dataset match the elements of the protected dataset. The attack ends when the criteria are met, indicating that the security of the model has been broken and obtaining a dataset which enables to impersonate a person.

3.1.2 Security Significance

(khandelwal & Chauhan, 2021) demonstrates the hugeness of security appeared differently in relation to various parameters of Cloud Computing.

(Pattnaik et al., 2022) In January 2010 an investigation charged by Microsoft for assessing miens on Cloud Computing which demonstrates 58% of the all group and about 86% of the bigger business organizations are basically used for capability of Cloud Computing.

3.1.3 Privacy

Sharing personal and sensitive information, some privacy protection techniques are proposed to solve problems. **(Filho & Gonçalves, 2020)** presented a modeling language and a novel structure with a structured process to address security and privacy barriers. The service provider will choose the purpose of the cloud provider.

When client data is adjusted by cloud and it is moved to another nation then they can get indistinct issues from delineated already. Close-by specialists could analyze the cloud providers in various areas to give the information of the cloud **(Swathi & Vani, 2020)**.

We have talked an extraordinary arrangement about the law in the past parts of this segment. Regardless of the way that as an affiliation you can have a not too bad organization agreement with any cloud supplier as still laws are there which can revoke some thinking. All type of people and affiliations are offered suitable registering which make it certain buying and selling of data viewing inappropriate acts. The customer records could be focused on its availability for specialists when they accept there is basic data put away in the cloud.

3.1.4 Security dangers

As there are diverse administrations in distributed computing there are likewise extraordinary secure impacts**(Filho & Gonçalves, 2020)**. The first to talk about is the SaaS secure. As we probably are aware at this point, with SaaS, organization data goes over the cloud. The organization or cloud supplier has a conventional database made reachable to the customer. At the point when customers need to acquire data shape, this database they are in charge of an application that can extricate it. There are not generally institutionalized organizations made accessible for acquiring information from the cloud. In the event that it is made, it is customized. This implies it isn't really good with different mists which help in making SaaS more secure. Change of data from all the cloud to various associations can be more exorbitant. Other type is known as PaaS. A programming interface can be provided to the client. For giving cloud programming the clients have to manage their services. This code isn't generally perfect with different stages of PaaS. The distinctions in preparing interfaces cause to frame the secure in light of the fact that the code should be reworked **(Filho & Gonçalves, 2020)**.

The last one of three is the IaaS. IaaS considered being more secure as till now no agreements have been made. All virtual machines and the product came in cloud as a package which is very much helpful in moving services to various mists. Suppliers of cloud don't just center around information convey ability for their clients.

Another renovation in cloud is known as distributed computing and so it can be termed as a new hazard**(Shawkat et al., 2022)**. Such things can imply that suppliers of cloud computing need to slow down their profession with issues from client side which came from light of cloud. Clients can then transfer their data to some other cloud provider with some different administration which can be clash and this needs to be revised. Sometimes such things can be the cause of client data loss. Against some downtime clients can be upheld.

Valuable services exhaustion can result into administration inaccessibility for the customer of cloud. Such results in their trading are unable to use for a particular measure of time. This off base relies upon its kind they are utilizing as a part of the cloud. Is it true that they are utilizing center occupation IT over the cloud or not. Another hazard can be classification of data over the cloud. This each and every single altogether result on the other hand in monetary, financial and reputational misfortunes **(Uhl & Rathgeb, 2021)**. Every one of the dangers that asset fatigue conveys to the table additionally represent some mechanical assaults from programmers.

In the first place there is the Lock as a result. This implies, in this situation, an association can't move its IT around to various specialist organizations. There are no institutional arrangements for distributed computing as it is new in the market. Also supplier can add trouble for any user to change to some another supplier **(khandelwal & Chauhan, 2021)**. Any customer or user can wind up services of cloud supplier. The customers IT can be pondered if any issue or problem will take place. Endeavoring and want to move their data to other cloud supplier can be very much expensive which would be impossible.

3.2 Related Work

In this research work we have presented on Cloud Data security enhancements through the biometric and encryption system.

(Imamverdiyev, 2009) presented a new feature extraction approach from fingerprints. This work particularly focused on extracting significant features from low-quality images. The technique added moderate noise to amplify a weak signal by using Stochastic resonance. The results showed that adding such a small amount of noise enhanced images that were of low-quality and aided in better extraction of features from such images.

(Sandhya et al., 2016) proposed a novel user authentication mechanism with fingerprint as the validation factor. The features were extracted based on the fingerprint textures by applying enhanced local line binary pattern. Probabilistic Neural Network was used for training and testing purposes. In addition to proposing a novel feature extraction, this method also attempted to salvage the missing portions of finger textures from the trained samples. Sensors supply raw picture collected from the individual to be authorized while algorithms related to signal processing does extraction of features from actual data while comparing algorithms should provide similarity for the data," claims **(Merhav, 2019)**. This concludes the decision-making process. Data fusion in multi-modal systems can be broken down into various levels, including feature level, score level, sensor level, and decision level. It is essential to examine the network in terms of biometric quality because different forms of fusion have varied effects on system performance.

(Dhane & Manikandan, 2021) proposed an intelligent cryptography mechanism for defending stored data from intruders in a cloud environment. This operated by dividing the data and distributing the fragments across cloud environment. This prevented intruders access to even partially available data. The experimental results proved that the method was both efficient and secured**. (Dhane & Manikandan, 2021)** proposed a security architecture for safe cloud transactions. The authors used one-time password mode of authenticating users. For securing communication, AES encryption was employed. This architecture was designed with an intent of providing security for all variety of services provided in cloud like SaaS, IaaS and PaaS. The results showed that the architecture ensured higher security in data exchange process.

A novel multimodal biometric system was proposed by**(Lee et al., 2021)** where four different traits viz., fingerprint, finger shape, knuckle points and finger vein were obtained from the hands of the users. The four traits were then combined at score level. The results of using four different traits with fusion at score level showed a significantly large distance between score distribution of users and imposters, in addition to yielding lower error rates.

In **(Haider, Rehman and Ali, 2020),** techniques for fusing biometrics and cryptography are discussed. Techniques for combining facial, fingerprint, and palm prints are suggested. Score They employed normalization in the multimodal biometric systems they deployed.

(Uhl & Rathgeb, 2021) provided a biometric based authentication mechanism for securing transactions and communication in cloud environment. In order to protect the sensitive biometric templates of users, the acquired templates were further encrypted to alleviate problems with theft of templates. Thus, the technique provided mechanism for secured transaction using authentication and protection of authentication information.

(Awasthi, 2022) presented a new fingerprint feature extraction technique that worked by tracing ridges during which, information in the context of ridges were collected. This helped in better identification of noisy regions. The experimental results revealed that the features extracted aid in better classification.

(El- El-Sofany, 2022) proposed a multiple biometric traits-based authentication on fingerprint and iris. Adaptive rank level fusion was employed for dynamic fingerprint and iris recognition.

(Wang et al., 2022) proposed a secured storage solution in cloud environment. It used encoding and forwarding operations on messages that were encrypted, in addition to providing re-encryption proxy mechanism. It also adopted erasure Coding for protecting the data, where data was divided into chunks, encoded and replicated over a distributed environment for safe storage. The technique enabled users to store data in cloud in a secured and robust way.

3.3 Literature Survey

The various sorts of studies are Literature reviews in the written form studies being research papers, Studies using Electronic Journals on Cloud Computing has been used during this study.

3.3.1 Biometric Authentication-Literature Survey

Biometric authentication validates users based on what they are. These are unique traits of users which can be both physiological and behavioral. These are one of the strong and reliable mode of authentication **(El- El-Sofany, 2022)**. There are number of advantages in using biometric traits like ease of use, difficult to forge, availability of credentials with supplicant and traits are highly unique. Unlike passwords, there is no way by which it can be forgotten or lost. These are like built-in passwords. To make the authentication mechanism even stronger, multiple traits can be acquired from the same user, clubbed and validated based on the traits. Such a mechanism is known as multimodal biometric authentication **(El- El-Sofany, 2022)**. Multimodal biometric systems are proved to have better accuracy than unimodal systems **(Uhl & Rathgeb, 2021)** and serves as better alternative to other modes of authentication **(Hossain and Al Hasan, 2020).**

Biometric authentication works by acquiring the biometric traits from users during registration and storing the template **(Manikandan, 2022)**. At the time of authentication, the user provided traits are compared with the stored templates. This is done by applying pattern recognition and matching algorithms. If the trait matches with the template, then requested access is allowed, else access is denied.

3.3.2 Encryption Algorithms- Literature Survey

(Wan, 2020) came up with a modified AES algorithm that could be applied to both text and images. The original AES algorithm's number of iterations were increased to 16. For rounds 1 to 15, the input plain text and keys were XORed, followed by substitution of bytes, shifting rows and mixing columns. For the final round, all operations excepting mixing columns were performed. The results proved that the modified AES algorithm, though increased the number of rounds, time it took to perform encryption was negligibly higher than that of original AES algorithm.

(Dhane & Manikandan, 2021) proposed a secured encryption algorithm that generated keys using genetic algorithm techniques. Genetic algorithm was employed to generate random numbers which serve as keys. The advantage of this was that these randomly generated number keys using genetic algorithm did not repeat and remained unique.

3.3.3 Cancellable Templates-Literature Survey

In **(Sandhya et al., 2016**) another approach of the cancellable templates model for protecting fingerprint minutiae templates is described. In this approach the analysis is performed in the domain of the extracted features and not in the signal domain. For the encryption of features is used a one-way function or non-invertible function, with the one-to-many property. The alignment process is performed by detecting the parabolic and triangular symmetry associated to the singular points of the fingerprint.

This pattern consists in a repeated and intentional distortion of the biometric signal based on a transformation **(Manikandan, 2022)**. The transformation has the fundamental property of non-invertibility of data. This type of transformation can be applied in both the domain of the signal and the extracted features of the biometric feature. The procedure for the transformation involves mapping the original characteristics S into S' so that it cannot be recovered S from S'. The function used to map the biometric features has the property of one to many and various functions can be used to perform the transformation of the other two components of a minutiae (y, σ).

3.3.4 Cryptographic Security-Literature Survey

The model proposed in **(Liu et al., 2019)** is composed by two methods, an encoding method and a decoding method of the fuzzy vault. The procedure performed to encode the biometric data is to create a generalized Reed-Solomon key word, representing the secret (along with the corresponding polynomial p where k represents the coefficients of the polynomial) **(Agrawal et al., 2022)**. The X coordinates corresponding to the original data set A are evaluated at p ← k. To hide the result of this operation, a set of garbage points or mockery spots are generated in the way (x, y) and mixed randomly. As premised, in the generation of garbage points, they should be selected in the way that do not to intersect in set A or the polynomial p. The method for decoding data contained in a fuzzy vault takes as input the sample set B at the vault Va and consists in determining the codeword encoding the secret k. If successful, the secret k is obtained as a result, which must be equal the original if the test set B is similar to the original set A.

According to several authors **(Mahmood & Tabassum, 2021)** the cryptographic security of this model is based on the computational difficulty of solving the problem of reconstructing the polynomial and the number of garbage points that are added to mask the original points.
In **(Mahmood & Tabassum, 2021)** an implementation of fuzzy vault model is performed and its cryptographic security is calculated using a key of 144 bits, of which 128 are used for encryption and 16 for code error correction. This attack aims to identify genuine points and garbage points inside the vault, to find a polynomial interpolation to obtain the original data. To consider a successful attack on a vault with 18 original points and 200 garbage points, is estimated that an average of 5.3 × 1010 attempts are required to find the amount of original points for a positive comparison.
An image is sent to the model as input to construct a 64-bit key in (**Muttaqin and Rahmadoni ,2020)** Generation of Biometric Key for Use in DES (2020). Using the binarization approach, the key is derived from the thinning of the image. The fingerprint may be improved further, and a variety of additional biometric information can be used to create the system with the highest level of security. It is suggested to use an efficient strategy or a generating cryptographic system.

(Agrawal et al., 2022) This protection method was proposed to perform the encryption fingerprint minutiae templates. The authors propose that the method has a security level of 85 bits for a system with strong personal entropy. To validate this level of security, they argue that to unlock a fuzzy vault is necessary to answer 29 questions out of 32 that were properly insured originally. This means, in biometric terms, that out of 32 minutiae that are in the original set, 29 have to compare positively with the sample set. Given that this protection method is proposed for applications that do not contain a high number of users, then the main problem is the amount of data to be compared by the comparison method. This causes the cryptographic security model to be variable, depending on the amount of comparison data. For example, the worst scenario would be finding a match of 1 in 6 million records. In this example, the security of the method is estimated to be 33 strength bits because it depends on the interpolation of a set of original features in the vault.
(Pranav & Dutta, 2022) This model is a cryptographic construction based on fuzzy compromise proposed in **(Pranav & Dutta, 2022)**. It is a biometric crypto-system designed to perform encryption of disorderly sets. The fuzzy vault model, first proposed in **(Agrawal et al., 2022)**, was conceived as an encryption method tolerant to fault.

3.4 Literature Review Matrix

Literature	**Summary**
(El- El-Sofany, 2022)	Biometric authentication validates users based on what they are. These are unique traits of users which can be both physiological and behavioral.
(Wan, 2020)	AES algorithm that could be applied to both text and images. The original AES algorithm’s number of iterations were increased to 16. For rounds 1 to 15, the input plain text and keys were XORed, followed by substitution of bytes, shifting rows and mixing

	columns. The results proved that the modified AES algorithm, though increased the number of rounds, time it took to perform encryption was negligibly higher than that of original AES algorithm.
(Dhane & Manikandan, 2021)	Intelligent cryptography mechanism for defending stored data from intruders in a cloud environment. This operated by dividing the data and distributing the fragments across cloud environment. This prevented intruders access to even partially available data. Genetic algorithm was employed to generate random numbers which serve as keys.
(Mahmood & Tabassum, 2021)	The cryptographic security of this model is based on the computational difficulty of solving the problem of reconstructing the polynomial and the number of garbage points that are added to mask the original points.
(Filho & Gonçalves, 2020)	Presented a modelling language and a novel structure with a structured process to address security and privacy barriers.
(Sandhya et al., 2016)	Cancellable templates model for protecting fingerprint minutiae templates is described. In this approach the analysis is performed in the domain of the extracted features and not in the signal domain. The alignment process is performed by detecting the parabolic and triangular symmetry associated to the singular points of the fingerprint.

4 Research Methodology

4.1 Research Method and Specification

Proposed System

Proposed architecture of biometric and encryption system

Security Architecture

The proposed security architecture secures data by ensuring safety at two levels viz., authentication and data. At the authentication level, the data is secured by allowing access only to genuine users and denying access to imposters (El- El-Sofany, 2022).

At the second level, data is secured by storing it in encrypted form, thus making the data unavailable to imposters. The integration factor of level 1 and level 2 is the crypto keys. The keys generated from multimodal features obtained at level I are used for encryption of data at level II.

Encryption algorithms use keys to encrypt and decrypt data. Encryption keys form the core for encrypting and decrypting data. For a known algorithmic procedure, it becomes easy to break the cipher text and get plain text if one manages to gain knowledge on the keys. Hence, a complex algorithmic encryption procedure coupled with unique and complex encryption keys make encryption extremely secure and hacker resistant.

As biometric traits are highly unique, usage of multiple modalities further increases uniqueness to the combination of traits. Keys for encrypting the cloud data are generated from these fused biometric traits and hence possibility of repetition of keys for encryption is very less. This makes the attempt to decrypt the files without having access to keys, highly complex. The proposed architecture and the Proposed system is shown in Figure 1 and Figure 2 respectively.

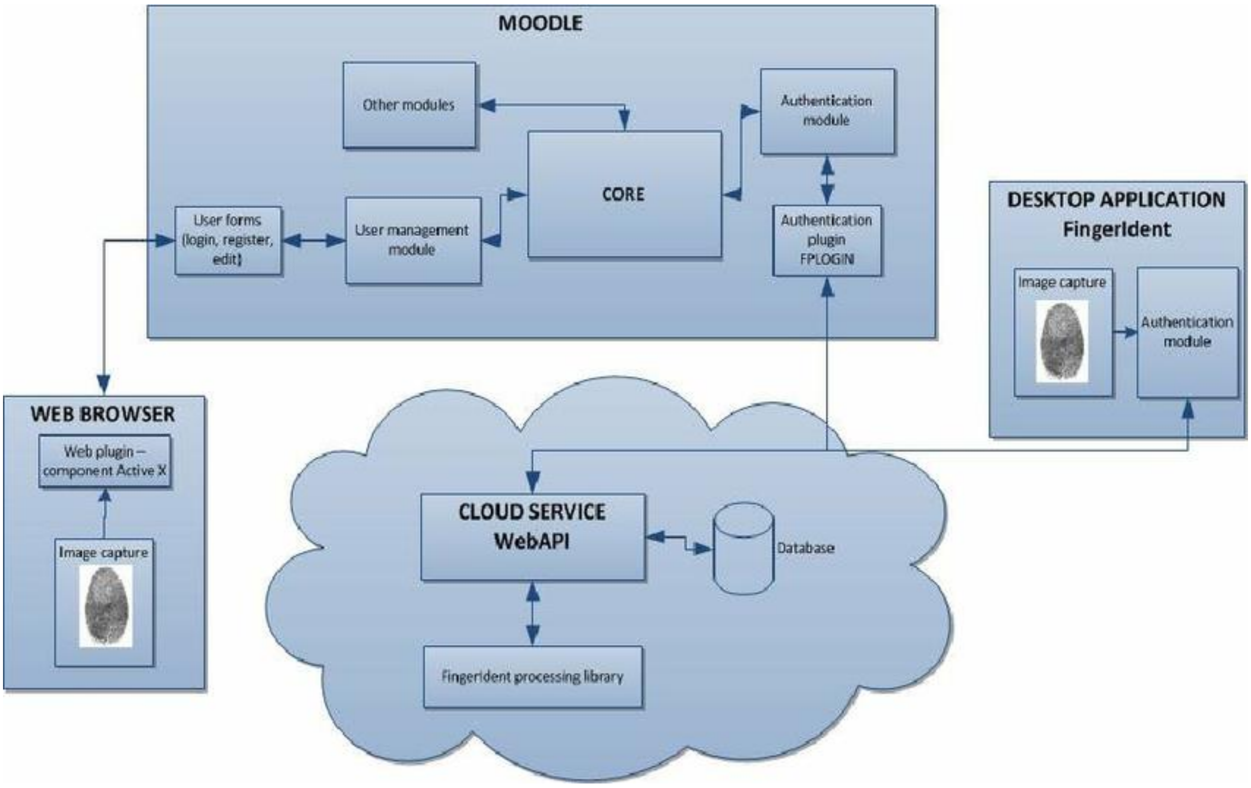

MOODLE
Other modules
CORE
Authentication module
User forms (login, register, edit)
User management module
Authentication plugin FPLOGIN
DESKTOP APPLICATION FingerIdent
Image capture
Authentication module
WEB BROWSER
Web plugin – component Active X
Image capture
CLOUD SERVICE WebAPI
Database
FingerIdent processing library

Figure 1. Proposed Architecture.

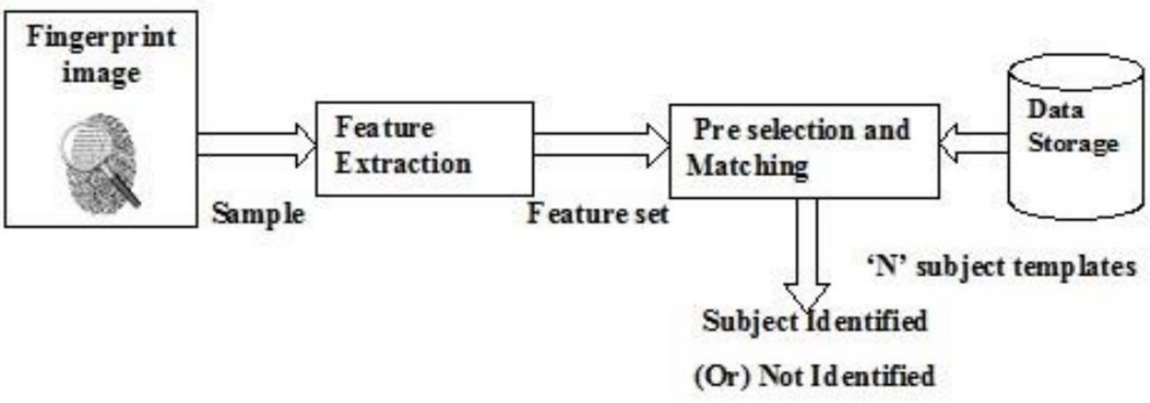


Figure 2. Proposed System or Flowchart

Feature Extraction

Most biometric systems have applications in forensic and verification systems. In forensic systems, fingerprints are used for identifying culprits in criminal activities. Verification systems include comparing the sample obtained from users with previously registered samples. For this purpose, it is essential to extract features from biometric images in a precise way. In any recognition system, feature extraction process plays a vital role **(Lee et al., 2021)** since the extracted features are used in matching the acquired traits with the registered traits.

Performing feature extraction on a pre-processed image results in features that are significant, thus, contributing to better accuracy of classification of a sample. Features are extracted based on number of parameters like texture, shape, contours etc. The choice of the technique depends on the outcome of applying the technique **(Bucur & Miclea, 2021)**.

Amazon: Amazon Web Services which include the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), and so on which give its client an exceptionally adaptable processing stage with more adaptability and accessibility

4.2 Research Design

4.2.1 Encryption

Encryption phase is used to transform plain text into cipher text and the corresponding decryption algorithm is used to convert cipher text into its respective plain text. The encryption process of the Pisces algorithm starts with input whitening, followed by sixteen rounds of Feistel cipher and ends with output whitening, the result of which is the cipher text. Within the sixteen-rounds, S-Box, Maximum Distance Separable (MDS) and Pseudo Hadamard Transformation (PHT) functions are carried out. In one single cycle, i.e., for every two rounds of Feistel Cipher, every bit of the given plain text is modified once.

4.2.2 Encryption Algorithms

The core of any encryption algorithm is key. Key and plain text become the input to the encryption algorithm. Encryption algorithms are of two types based on the type of keys used viz., symmetric key algorithm and asymmetric key algorithm.

In asymmetric encryption technique **(Dhane & Manikandan, 2021)**, the sender encrypts with a key known as the public key and the receiver decrypts with another key called private key. Thus, two different keys are used. This type of algorithm is also known as public key encryption.

4.2.3 Encryption Keys

The central principle of encryption is the encryption key used to perform the operation.

4.3 Scope Of the Research

The targeted users of the proposed research work include users who opt for data storage and retrieval in cloud. The users would also cover service providers who provide data storage services in cloud. Among various services available in cloud, the scope is limited to cloud users who avail services for storing data.

4.4 Implementation

Samples of the biometric or fingerprint images are taken from the available database.

4.4.1 Biometric Key Generation

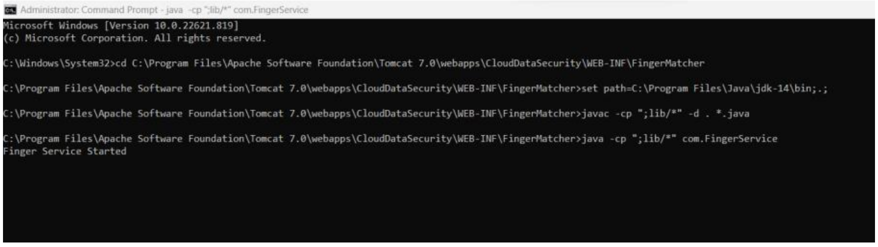
The fingerprint image is first processed to extract the fingerprint's key details. The accessibility of affordable, portable stable scanners and the availability of significant fingerprint similarities are two crucial factors in the use of these identification techniques. In our research paper, we are accepting only fingerprint image as the biometric input. Fingerprint image is considered a better authentication process during login because it is a unique, biometric characteristic that can be easily and quickly scanned. Additionally, it is difficult to forge or replicate a fingerprint, making it a secure method of identifying an individual. Fingerprint authentication is also convenient as it eliminates the need for users to remember and enter a password, reducing the risk of password-related security breaches. The proposed research aims to utilize fingerprints as a means of improving security. The use of fingerprints is preferred as the method of collecting this biometric information is non-invasive.

4.4.2 Biometric Properties

To properly compare a biometric with a previously stored trait, the following biometric attributes must be preserved.

- Biometrics ability to maintain consistency over a long length of time is known as invariance.
- The biometric template's ability to be measured quickly determines Measurability as well as Timeliness.
- The trait of biometrics being distinctive is referred to as Singularity.
- Reducibility - The ability of biometrics to be smaller so that storage is simple.
- Reliability - The biometric must be accurate, and the individual's privacy shouldn't be compromised.

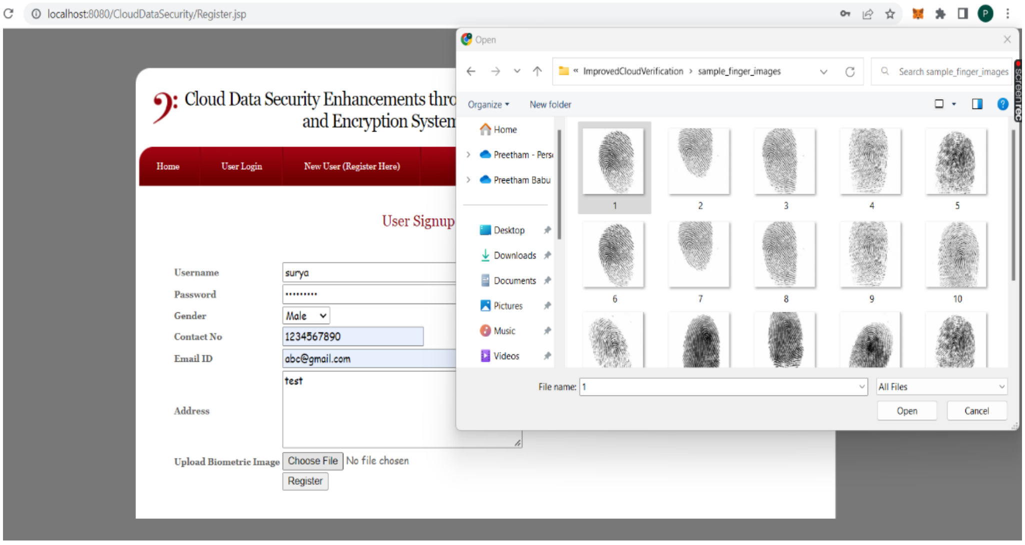
In the proposed work the fingermatch service is run so as to when the user sign ups with a fingerprint, the minutiae extraction points are collected through the fingermatch service. The keys are generated providing the level of security. When the user tries to login to the system, these extraction points help in matching the correct fingerprint to authenticate the user. Java is used in order to run this service. Respective jars and libraries are downloaded. The Fingermatch service is run to match the biometric for sign up and signing in. It is as shown in Figure 3.



```
Administrator: Command Prompt - java  -cp ";lib/*" com.FingerService
Microsoft Windows [Version 10.0.22621.819]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\CloudDataSecurity\WEB-INF\FingerMatcher

C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\CloudDataSecurity\WEB-INF\FingerMatcher>set path=C:\Program Files\Java\jdk-14\bin;.;

C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\CloudDataSecurity\WEB-INF\FingerMatcher>javac -cp ";lib/*" -d . *.java

C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\CloudDataSecurity\WEB-INF\FingerMatcher>java -cp ";lib/*" com.FingerService
Finger Service Started
```

Figure 3. Fingermatch service started

A user gives the system with biometric samples during the registration step. To create the key, two samples are now used, and a third (belonging from different modality) is utilized to verify the user. The following procedures are carried out during the enrolment phase. Figure 4. shows the registration phase where sensor gathers the biometric information and Preprocessed data is used to extract features. The biometric template is used to create a cryptographic key after the two biometrics have been combined.



localhost:8080/CloudDataSecurity/Register.jsp

Cloud Data Security Enhancements thro
and Encryption Systen

User Signup

Username	surya
Password	•••••••••
Gender	Male
Contact No	1234567890
Email ID	abc@gmail.com
Address	test
Upload Biometric Image	Choose File No file chosen

File name: 1

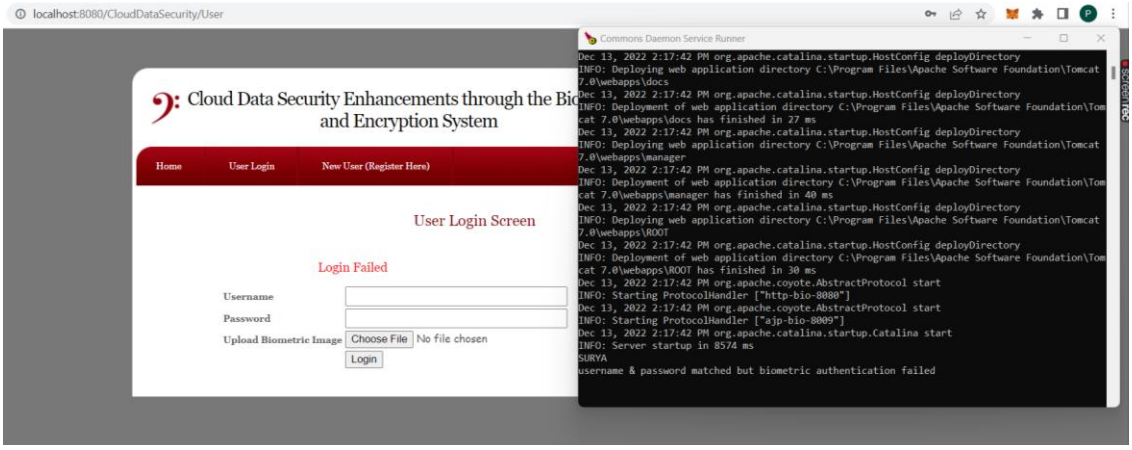
Fig 3.4 Registration Phase

The verification process begins with the user providing three biometric samples, which are then translated to an encryption key. Biometric images are used to create the generated encrypted keys and cancellable biometric pattern. The key is withheld if the encrypted key doesn't replicate the one in the memory unit, and the user is required to resubmit his biometric data. A similarity score is determined between the resulted cancellable biometric data and with the one identified in the look-up database corresponding to the encrypted key if a matching key is identified. This will authenticate or provide access to the user to login into the system.

Authentication is only given if

- Biometric image is matched with the encrypted key found in the look-up table.
- Similarity score is above or matching the predefined limit.

Figure 5 shows the error if the biometric image doesn't match during the login.


localhost:8080/CloudDataSecurity/User
Commons Daemon Service Runner
Home
User Login
New User (Register Here)
Choose File
Login
screenrec

Cloud Data Security Enhancements through the Bic and Encryption System

User Login Screen

Login Failed

Username

Password

Upload Biometric Image No file chosen

```
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\Program Files\Apache Software Foundation\Tomcat
7.0\webapps\docs
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\Program Files\Apache Software Foundation\Tom
cat 7.0\webapps\docs has finished in 27 ms
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\Program Files\Apache Software Foundation\Tomcat
7.0\webapps\manager
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\Program Files\Apache Software Foundation\Tom
cat 7.0\webapps\manager has finished in 40 ms
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\Program Files\Apache Software Foundation\Tomcat
7.0\webapps\ROOT
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\Program Files\Apache Software Foundation\Tom
cat 7.0\webapps\ROOT has finished in 30 ms
Dec 13, 2022 2:17:42 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-bio-8080"]
Dec 13, 2022 2:17:42 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["ajp-bio-8009"]
Dec 13, 2022 2:17:42 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 8574 ms
SURYA
username & password matched but biometric authentication failed
```

Figure 5. Login error when there is mismatch in the biometric Image chosen.

5 Evaluation

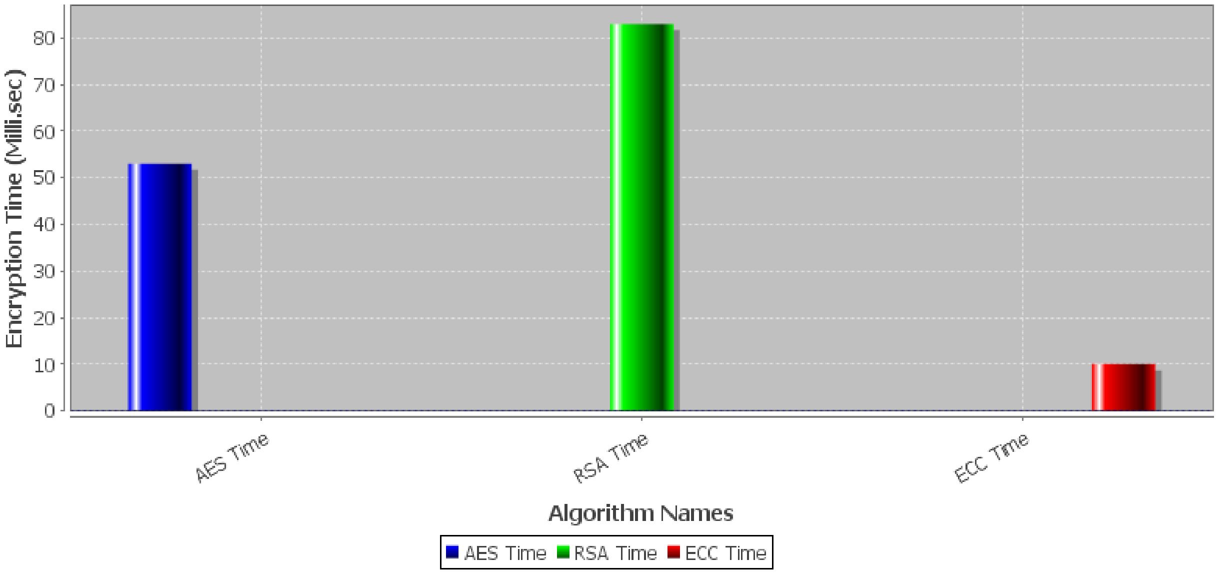


Figure 6. Computation Time graph on Comparison of cryptographic AES,RSA and ECC algorithms

As shown in Figure 6 the encrypted format of the file uploaded is displayed on 'Computation Time Graph'. In the above comparison graph x-axis represents algorithm names and y-axis represents Computation time of those algorithms in Milli Seconds. We experimented with 3 different encryption algorithms such as AES, RSA and ECC and their performance was evaluated in terms of computation time and depending on the size of the file uploaded.

5.1 Experiment/Case study

To test the application, we shall login safely using biometrics. After the data is being uploaded to the cloud, the file is checked to determine if it was correctly encrypted. The uploaded file should be uploaded to the AWS S3 bucket of the user account that is linked with the Secret access key.

In Case Study 1, the text document (.txt file) source file that needs to be uploaded to the cloud storage service is analyzed. After decrypting the file, the decryption's success is verified. The Encrypted text file as shown in the Figure 7.

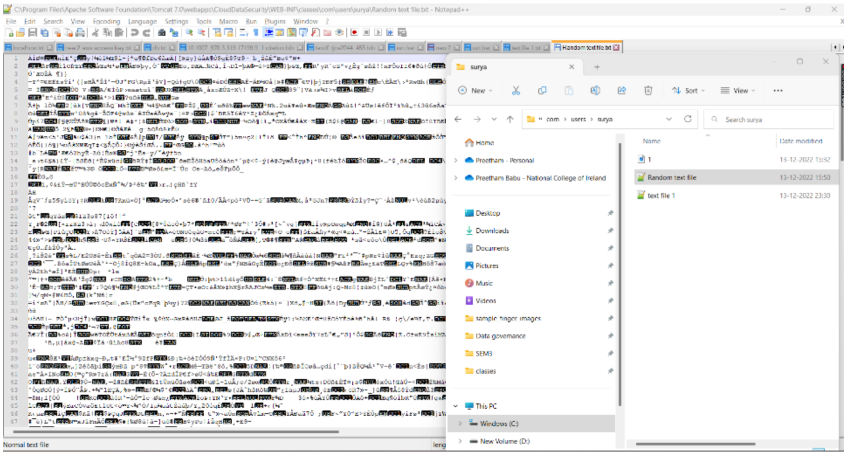
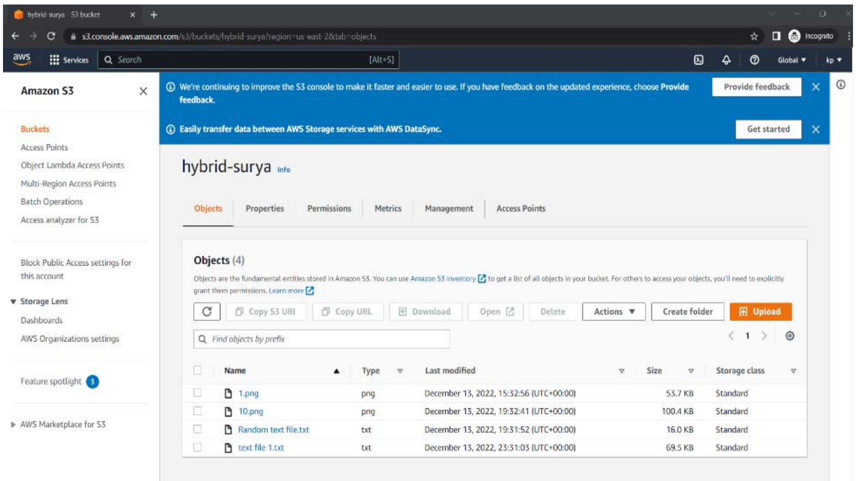


Figure 7. Encrypted Text file

The uploaded file will get into Amazon S3 bucket as shown in Figure 8.



We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.

Easily transfer data between AWS Storage services with AWS DataSync.

hybrid-surya

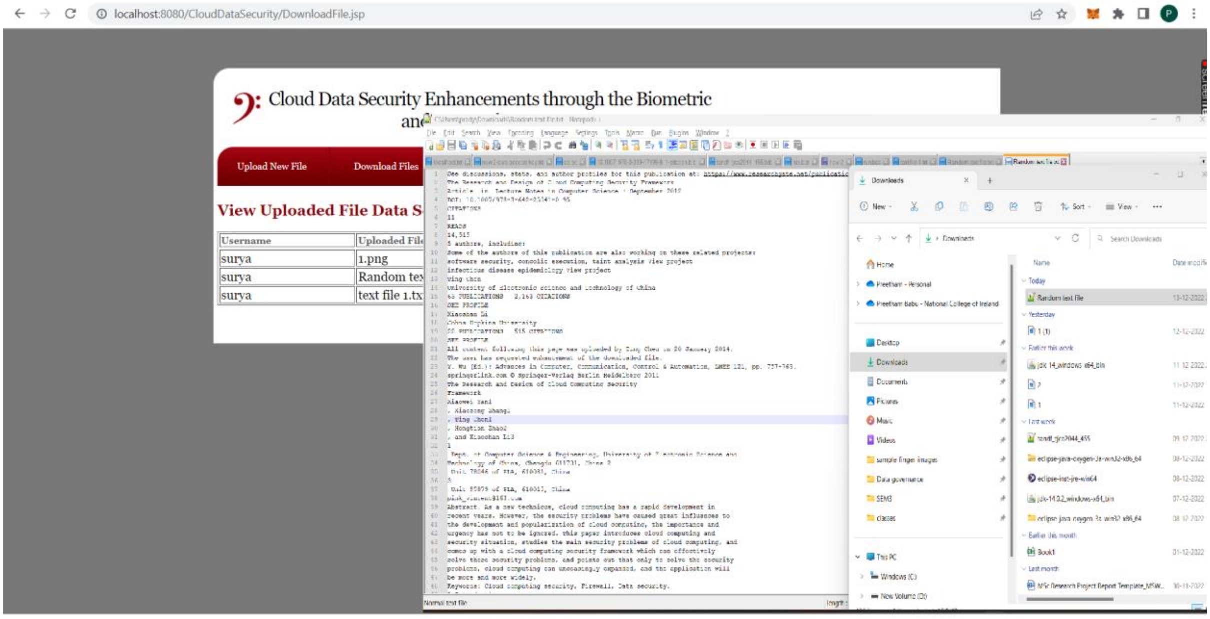
Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
1.png	png	December 13, 2022, 15:32:56 (UTC+00:00)	53.7 KB	Standard
10.png	png	December 13, 2022, 19:32:41 (UTC+00:00)	100.4 KB	Standard
Random text file.txt	txt	December 13, 2022, 19:31:52 (UTC+00:00)	16.0 KB	Standard
text file 1.txt	txt	December 13, 2022, 23:31:03 (UTC+00:00)	69.5 KB	Standard

Figure 8. File uploaded to AWS S3 bucket.

The decrypted file after downloading will be as shown in Figure 9.


localhost:8080/CloudDataSecurity/DownloadFile.jsp
Cloud Data Security Enhancements through the Biometric
an
Upload New File
Download Files
View Uploaded File Data S
Downloads
Home
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Normal text file

Username	Uploaded Fil
surya	1.png
surya	Random tex
surya	text file 1.tx

```
See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publicatio
The Research and Design of Cloud Computing Security Framework
Article in Lecture Notes in Computer Science · September 2012
DOI: 10.1007/978-3-642-25541-0_95
CITATIONS
11
READS
14,515
5 authors, including:
Some of the authors of this publication are also working on these related projects:
software security, concolic execution, taint analysis View project
infectious disease epidemiology View project
Ying Chen
University of Electronic Science and Technology of China
63 PUBLICATIONS   2,163 CITATIONS
SEE PROFILE
Xiaochen Li
Johns Hopkins University
22 PUBLICATIONS   515 CITATIONS
SEE PROFILE
All content following this page was uploaded by Ying Chen on 20 January 2014.
The user has requested enhancement of the downloaded file.
Y. Wu (Ed.): Advances in Computer, Communication, Control & Automation, LNEE 121, pp. 757-763.
springerlink.com © Springer-Verlag Berlin Heidelberg 2011
The Research and Design of Cloud Computing Security
Framework
Xiaowei Yan1
, Xiaosong Zhang1
, Ting Chen1
, Hongtian Zhao2
, and Xiaochan Li3
1
 Dept. of Computer Science & Engineering, University of Electronic Science and
Technology of China, Chengdu 611731, China 2
 Unit 78046 of PLA, 610031, China
3
 Unit 55879 of PLA, 610031, China
pink_vincent@163.com
Abstract. As a new technique, cloud computing has a rapid development in
recent years. However, the security problems have caused great influences to
the development and popularization of cloud computing, the importance and
urgency has not to be ignored. this paper introduces cloud computing and
security situation, studies the main security problems of cloud computing, and
comes up with a cloud computing security framework which can effectively
solve these security problems, and points out that only to solve the security
problems, cloud computing can unceasingly expanded, and the application will
be more and more widely.
Keywords: Cloud computing security, Firewall, Data security.
```

Figure 9. Decrypted Text file.

Similarly the experiment was carried out on different file type(.jpg/.png) and on different file sizes and the observations were recorded. It is found that in this experiment, the AES encryption algorithm has an upper hand over the other two algorithms RSA and ECC in terms of the computation time. AES encryption method takes less time compared to other two encryption methods.

Initially we tested with a text file of 16kb as the code was running on local. If the size of the file is more(>100kb), then it would take more time to get encrypted. I have tested for different file types (img, png, pdf, docs, txt) and different file sizes (up to 1 MB) and the encryption works well with these set of algorithms. However, the system is scalable when it is on cloud environments. The fingerprint image uploaded during the sign up are about 70kb and this fingerprint image would be uploaded to AWS S3 bucket in order to verify the login process. I also uploaded an image file of more than 90kb and checked the results and encryption algorithms were working fine. The algorithms would display different computation times based on the different file types and file size that are uploaded to the cloud. The key pairs have been imported in the java files for different algorithms and their files.

For example – In AES encryption, the following libraries are imported to get the keypair.

```
import javax.crypto.KeyGenerator;
import javax.crypto.spec.SecretKeySpec;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
```

5.2 Analysis

5.2.1 Results And Discussion

This research covers design of biometric and encryption system protocol, algorithms and methodologies. The very first application was the secure storage of biometric images which includes fingerprint images.

To develop an encryption algorithm to make the communication is secure one to use of genetic algorithm in stream cipher to reduce the cost and time to encrypt the information with increased security.

The algorithm is evaluated by using the sample input and varying keys that differ by 1 bit. An input string is encrypted using a key and cipher text is generated. The same input with another key that differs from the previous key is again used to encrypt the text. Avalanche effect is thus calculated by finding the difference in the number of bits that are flipped in both the outputs.

Authentication and security is required very much to enable the person to gain access to a private and confidential data. The biometric techniques can be used for the authenticity of a person. The security of these biometric traits can be achieved through cryptography **(Shirgaonkar et al., 2022)**. Generation of attribute based relative key for the stream cipher encryption to improve the security of the information. Generation of different encryption key for the session based service oriented flow estimated key selection approach. **(Anon & Tyagi, 2021)** The non-biased group proposed privacy with a plan for securing signatures. It provides anonymous access to various services and cloud environment servers. This ensures the integrity and accuracy of the spreading data using AES symmetric gravity. If a user was found, there was something wrong with the services, and his access was canceled by a manager. We have compared the performance of the encryption algorithms. The AES encryption algorithm has an upper hand over the other two algorithms RSA and ECC in terms of the computation time. AES encryption method takes less time compared to other two encryption methods.

5.3 Contributions: Research achievements and achieved results.

Contribution of the Research

There are two spectrums of security requirement in cloud environment viz., one from service providers' end and the other from the users' end. This requirement is addressed in the proposed research work.

The objective Cloud Data security enhancements through the biometric and encryption system is achieved by providing an architecture for authentication of users and a method for securely storing user's data.

Data and information possess important characteristics which are essential for ensuring security **(Abdul et al., 2017).** There are five important characteristics, viz., availability, accuracy, authenticity, confidentiality and integrity **(Filho & Gonçalves, 2020).**

Availability: The stored data should be accessible by authorized users without any difficulty. In addition to availability, the data should also be in a format that is required.

Accuracy: The data that is stored should be error-free when retrieved. The accuracy aspect of data is lost if the data retrieved varies grossly with the stored data.

Authenticity: The data that is accessed should be the original one. The retrieved data should be free from any fabrication.

Integrity: The data that is stored should remain unchanged and unmodified and should be complete. Any minute modification will result in loss of integrity of data.

Confidentiality: The data is considered to be confidential when the stored data is protected from unauthorized access. This can be further ensured by laying down strict access control and access rights policy.

6 Conclusion

In this thesis research report researcher to build Cloud Data security enhancements through the biometric and encryption authentication system where user can sign up with biometric data and after correct login they can upload any file and all files will be uploaded to Amazon in encrypted format and biometric data will also be saved in Amazon S3 bucket in encrypted format. Researcher experimented with 3 different encryption algorithms such as AES, RSA and ECC and their performance was evaluated in terms of computation time.

The following is a succinct summary of the work's primary contributions:

- It is suggested to use fingerprints as a biometric with effective fusion and a reliable key mechanism.
- A safe framework with 0% erroneous acceptance rate and privacy for biometric templates is suggested.
- It is advised to use secure file uploading and downloading methods when using the cloud.

References

Abdul, W. et al. (2017) “Biometric security through visual encryption for Fog edge computing,” IEEE Access, 5, pp. 5531–5538. Available at: https://doi.org/10.1109/access.2017.2693438.

Agrawal, S., Yadav, A. and Yamada, S. (2022) “Multi-input attribute based encryption and predicate encryption,” Advances in Cryptology – CRYPTO 2022, pp. 590–621. Available at: https://doi.org/10.1007/978-3-031-15802-5_21.

Ali, H., 2015. Cloud Computing Security: An Investigation into the Security Issues and Challenges Associated with Cloud Computing, for both Data Storage and Virtual

Applications. International Research Journal of Electronics and Computer Engineering, 1(2), p.15.

Amedzro St-Hilaire, W. (2020) “National frameworks for the implementation of Digital Security,” Digital Risk Governance, pp. 11–22. Available at: https://doi.org/10.1007/978-3-030-61386-0_2.

Anon, P. and Tyagi, S.S. (2021) “Enhancing security of cloud data through encryption with AES and fernet algorithm through convolutional-neural-networks (CNN),” International Journal of Computer Networks and Applications, 8(4), p. 288. Available at: https://doi.org/10.22247/ijcna/2021/209697.

Awasthi, L. (2022) “Data Security in cloud computing using hybrid encryption algorithms,” INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 06(05). Available at: https://doi.org/10.55041/ijsrem13299.

Bucur, V. and Miclea, L. (2021) “Optimizing towards a multi-cloud environment through benchmarking data transfer speeds in Amazon Web Services and google cloud,” 2021 IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP) [Preprint]. Available at: https://doi.org/10.1109/iccp53602.2021.9733705.

Dhane, H. and Manikandan, V.M. (2021) “A new framework for secure biometric data transmission using block-wise reversible data hiding through encryption,” 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS) [Preprint]. Available at: https://doi.org/10.1109/icds53782.2021.9626742.

El- El-Sofany, H. (2022) “A proposed biometric authentication model to improve cloud systems security,” Computer Systems Science and Engineering, 43(2), pp. 573–589. Available at: https://doi.org/10.32604/csse.2022.024302.

Filho, E. and Gonçalves, V. (2020) “Achieving privacy, security, and interoperability among biometric networks using symmetric encryption,” Proceedings of the 6th International Conference on Information Systems Security and Privacy [Preprint]. Available at: https://doi.org/10.5220/0008961504810489.

Herre, T. (2020) “Simplifying secure cloud computing environments with Cloud Data Centers,” Cloud Computing Security, pp. 411–424. Available at: https://doi.org/10.1201/9780429055126-35.

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

Hidayat, T., 2019. ENCRYPTION SECURITY SHARING DATA CLOUD COMPUTING BY USING AES ALGORITHM: A SYSTEMATIC REVIEW. TEKNOKOM, 2(2), pp.11-16.

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.

Imamverdiyev, Y.N. (2009) “A biohashing method for fingerprint templates protection,” 2009 International Conference on Application of Information and Communication Technologies [Preprint]. Available at: https://doi.org/10.1109/icaict.2009.5372543.

khandelwal, Y. and Chauhan, K. (2021) “Biometric identification for Advanced Cloud Security,” Deep Learning Approaches to Cloud Security, pp. 167–187. Available at: https://doi.org/10.1002/9781119760542.ch11.

Lee, M.J. et al. (2021) “A tokenless cancellable scheme for multimodal biometric systems,” Computers & Security, 108, p. 102350. Available at: https://doi.org/10.1016/j.cose.2021.102350.

Le, D.N., Pal, S. and Pattnaik, P.K., 2022. Reliability Issues in Cloud Computing Environment. Cloud Computing Solutions: Architecture, Data Storage, Implementation and Security, pp.103-121.

Mahmood, M.A. and Tabassum, T. (2021) “A hybrid cryptographic data security system utilizing Fuzzy Vault Key,” 2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON) [Preprint]. Available at: https://doi.org/10.1109/raaicon54709.2021.9930051.

Manikandan, V.M. (2022) “A secure biometric authentication system for smart environment using reversible data hiding through encryption scheme,” Machine Learning for Biometrics, pp. 201–216. Available at: https://doi.org/10.1016/b978-0-323-85209-8.00002-x.

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.

Nishiuchi, N. and Soya, H. (2011) “Cancelable biometric identification by combining biological data with artifacts,” 2011 International Conference on Biometrics and Kansei Engineering [Preprint]. Available at: https://doi.org/10.1109/icbake.2011.11.

Pranav, P. and Dutta, S. (2022) “Design of a fuzzy rule based expert system for automatic raga selection for cryptographic applications.” Available at: https://doi.org/10.21203/rs.3.rs-1163172/v1.

Reddy, P., Sam, R. and Bindu, C., 2016. Optimal Blowfish Algorithm based Technique for Data Security in Cloud. International Journal of Business Intelligence and Data Mining, 1(1), p.1.

Sandhya, M., Prasad, M.V.N.K. and Chillarige, R.R. (2016) “Generating cancellable fingerprint templates based on Delaunay triangle feature set construction,” IET Biometrics, 5(2), pp. 131–139. Available at: https://doi.org/10.1049/iet-bmt.2015.0034.

Shawkat, S.A., Tuama, B.A. and Al_Barazanchi, I. (2022) “Proposed system for data security in Distributed Computing in using triple Data Encryption Standard and rivest Shamir adlemen,” International Journal of Electrical and Computer Engineering (IJECE), 12(6), p. 6496. Available at: https://doi.org/10.11591/ijece.v12i6.pp6496-6505.

Shirgaonkar, M. et al. (2022) “Cloud computing security using cryptographic algorithms,” 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) [Preprint]. Available at: https://doi.org/10.1109/iccmc53470.2022.9753711.

Singh, G. and Garg, S. (2020) “Fuzzy elliptic curve cryptography based cipher text policy attribute based encryption for cloud security,” 2020 International Conference on Intelligent Engineering and Management (ICIEM) [Preprint]. Available at: https://doi.org/10.1109/iciem48762.2020.9159961.

Smith, M., Mann, M. and Urbas, G. (2018) “Biometrics in criminal trials,” Biometrics, Crime and Security, pp. 85–111. Available at: https://doi.org/10.4324/9781315182056-6.

Swathi, V. and Vani, M.P., 2020, July. Privacy-Cheating Discouragement: A New Homomorphic Encryption Scheme for Cloud Data Security. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

T., M., 2020. ECSORRMAN: Optimal Random Route Selection and Elliptic Curve Cryptography Based Security Schema for Mobile ADHOC Network. Journal of Advanced Research in Dynamical and Control Systems, 51(SP3), pp.409-419.

Uhl, A. and Rathgeb, C. (2021) “Biometric encryption,” Encyclopedia of Cryptography, Security and Privacy, pp. 1–6. Available at: https://doi.org/10.1007/978-3-642-27739-9_1519-1.

Wan, A., 2020. A Robust Cloud Security Architecture based on Distributed Servers, User Authentication, and AES, Blowfish Encryption Techniques. Journal of Advanced Research in Dynamical and Control Systems, 12(SP3), pp.1293-1300.

Wan, A.R. (2020) “A robust cloud security architecture based on distributed servers, User Authentication, and AES, Blowfish Encryption Techniques,” Journal of Advanced Research in Dynamical and Control Systems, 12(SP3), pp. 1293–1300. Available at: https://doi.org/10.5373/jardcs/v12sp3/20201378.

Wang, G., Liu, Q., Wu, J. and Guo, M., 2011. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security, 30(5), pp.320-331.

Wang, R., Miao, F. and Yu, Y. (2022) “PRE-DAC: Proxy re-encryption based dynamic access control for Secure Cloud Data,” International Conference on Network Communication and Information Security (ICNCIS 2022) [Preprint]. Available at: https://doi.org/10.1117/12.2657100.

Wichmann, P. et al. (2021) “Detection of brute-force attacks in end-to-end encrypted network traffic,” The 16th International Conference on Availability, Reliability and Security [Preprint]. Available at: https://doi.org/10.1145/3465481.3470113.

Yao, Z. et al. (2015) “Blind minutiae selection for standard minutiae templates,” IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015) [Preprint]. Available at: https://doi.org/10.1109/isba.2015.7126367.

Zhao, Z. and Xu, X. (2022) “Research on the application of Computer Data Encryption Technology in cloud security,” International Journal of Engineering and Technology, 14(4), pp. 75–78. Available at: https://doi.org/10.7763/ijet.2022.v14.1206.