A PROJECT REPORT ON

ENCRYPTION OF CLOUD DATA USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF ENGINEERING (COMPUTER ENGINEERING)

SUBMITTED BY

STUDENT NAME	EXAM NO.
Ayush Bolla	B190074209
Deep Pawar	B190074255
Pranit Rathod	B190074258
Vishaka Matkar	B190074243

Under the guidance of

Prof. D. D. Sapkal

DEPARTMENT OF COMPUTER ENGINEERING

PVG's COLLEGE OF ENGINEERING AND TECHNOLOGY & G K PATE(WANI) INSTITUTE OF MANAGEMENT

44, VIDYANAGARI, PARVATI, PUNE 411009

SAVITRIBAI PHULE PUNE UNIVERSITY

2022-23

CERTIFICATE

This is to certify that the project report entitles

"ENCRYPTION OF CLOUD DATA USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY"

Submitted by

STUDENT NAME	EXAM NO.
Ayush Bolla	B190074209
Deep Pawar	B190074255
Pranit Rathod	B190074258
Vishaka Matkar	B190074243

is a bonafide student of this institute and the work has been carried out by him/her under the supervision of Prof. D D Sapkal and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of Bachelor of Engineering (Computer Engineering).

Prof. D. D. Sapkal	**Prof. D. D. Sapkal**	**Dr. M R Tarambale**
Guide	Head of Department	I/C Principal,

Place: Pune

Date:

Acknowledgement

It gives us great pleasure in presenting the Project Work - I report on "Encryption of cloud data using hybrid cryptography and steganography" and to express my deep regards towards those who have offered their valuable time and guidance in our hour of need.

I would like to express my sincere and wholehearted thanks to our project guide and Head of the department Prof. D.D.Sapkal for contributing valuable time, knowledge, experience and providing valuable guidance in making this project a success

I am also glad to express my gratitude and thanks to our Principal Prof. Manoj R. Tarambale Sir for their constant inspiration and encouragement. Finally, before ending I would like to express my gratitude and thanks to all my colleagues who are involved directly and indirectly in making this project a success.

Ayush Bolla
77

Deep Pawar
79

Pranit Rathod
13

Vishakha Matkar
07
(B. E. Computer Engineering)

Abstract

More quickly than ever, the modern world is expanding, and new technologies and discoveries are making people's lives easier than before. The security of one's online data is a key difficulty that the majority of people encounter as a result of new technological breakthroughs. When consumers save their data online on cloud servers, they still face this security problem. Cryptography can be used to help solve the problem. Cloud computing has become increasingly important in recent years in the computing industry. The way computers are utilised in the sector has been transformed from first putting up the framework and then employing it to just calling up the resources from various cloud vendors as needed. It is also utilised in several businesses for a variety of services and data storage. Users can request the retrieval of their data from the cloud, but many users are worried about the privacy and safety of their data. Techniques like steganography and cryptography can be used to address the security issue that most consumers are worried about.

In order to secure the data, cryptographic methods like AES as well as RSA are utilised, but occasionally employing only one method doesn't result in high security. In this article, we have concentrated on providing a hybrid cryptographic process that uses a variety of methods to encrypt and decode data. The suggested system uses the AES and ECC techniques to ensure security. There are three sections to the encryption in this place. When necessary, each component is encrypted using a distinct encryption technique and decrypted using a different key.By employing AES and ECC to store encrypted information on a single cloud server, this encryption and decryption system provides users with enhanced data security. After that, the LSB method will be used to conceal the encrypted data within an image. We employ the SHA hashing method throughout the data validation stage. Additionally, in our proposal, the data is compressed with the LZW technique before being concealed in the image. As a result, it enables the maximum amount of data concealing. We can accomplish strong data security by utilising this information concealment technologies and hybrid encryption.

List of Abbreviations

ABBREVIATION	ILLUSTRATION
AES	Advanced Encryption Standard.
ECC	Elliptic Curve Cryptography
LSB	Least-Significant Bit
LZW	Lempel–Ziv–Welch
SHA	Secure Hash Algorithms
RSA	Rivest Shamir Adleman
IoT	Internet of Things
SRS	Software Requirements Specification
LAN	Local Area Network
WAN	Wide Area Network
HTTP	Hypertext Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
RNG	Random Number Generator
SDLC	Software Development Life Cycle
DFD	Data Flow Diagram
UML	Unified Modeling Language
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Square Error
SSIM	Structural Similarity Index Matrix

Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1. OVERVIEW

One of the significant developments in data innovation is cloud setup, but in the cloud conditions, the safety issue of data storing is a major challenge. This suggested system provides a framework that makes use of encryption, data hiding, and hashing capabilities to address this problem. At the data encryption stage, we carried out cross-breed encryption employing the computations of AES symmetrical encryption with ECC key encryption.

1.2. MOTIVATION

Information technology recently underwent a dramatic change that is mostly credited to cloud computing. Cloud storage has emerged as one of the most popular and important services due to the growing use and processing of information in most institutions, governments, banks, etc. Instead of using a computer's hard drive, cloud computing allows users to access and save data and programmes over the internet. Users can read paperwork and use application from any device with an internet connection. Today, research on safety in cloud computing is a developing topic. The vast majority of businesses are switching from outdated practises like physical storage of information to cloud storage, which offers convenient access to data anytime, anywhere. However, one of the major challenges in implementing cloud computing for businesses is data security.

The development of technology has raised the value of both software and hardware as well as increased internet usage. As recompense for each time they are used, clients of cloud computing are given access to a pooling of resources and services. As a result, it has grown in popularity since it makes resources available online, maximising both user time and money.

The primary objective of our project is to protect client data at the cloud storage plus client side from various sorts of attackers by utilising the symmetric key cryptography technique.

1.3. PROBLEM DEFINITION

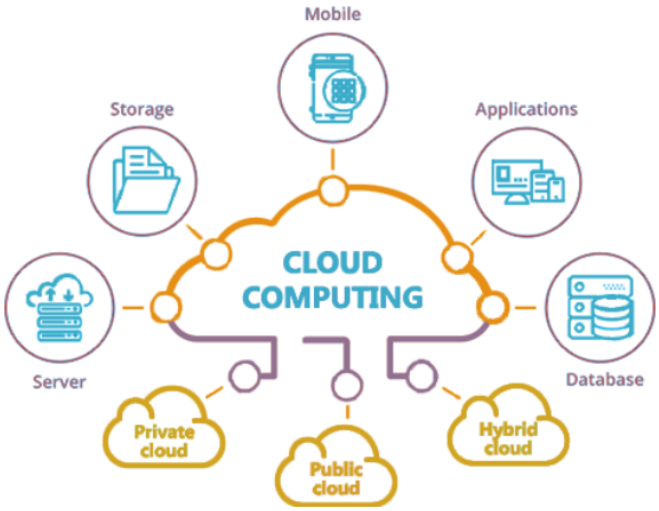
Cloud computing is one of the important developments in information technology, but in a cloud setting, the safeguarding issue of data storage is a major issue. The efficiency, security, and efficiency of the entire system are all impacted by design difficulties with the cloud as a method of supplying computer resources.

Through IP addresses, devices communicate with one another over the internet. Right now, the IoT is just getting started. In the upcoming years, it will have an impact on how we

live our daily lives. The risk of technology being abused will increase as it becomes increasingly ingrained into our way of life.

The IoT ecosystem faces many significant security concerns, including privacy leakage, eavesdropping, and unauthorized access. Data during transmission must be fiercely protected right away. In order to increase the privacy of cloud data, a system employing hashing, encryption, and information concealment is suggested in this work. A hybrid cryptography technique is suggested in order to accomplish anonymity and boost security in internet-based communications.

Figure 1: Cloud Computing



1.4 PROJECT SCOPE AND LIMITATIONS

1.4.1 Project Scope

Cloud computing is currently being used to store massive amounts of data. Whenever a user requests data from the cloud, we can retrieve it. While storing data securely across the cloud, there are numerous problems that arise. Using hybrid cryptography, these problems can be resolved. The suggested architecture is a hybrid model that combines each of the algorithm's AES with ECC for storing confidential data or data produced by IoT devices over the cloud. ECC is used to generate keys for the encryption of data in AES. Simply said, we produce the key using the ECC technique rather than the AES approach because it has a smaller key size. The public or a private key is used for data encryption and decryption, just like in symmetric/asymmetric encryption. As a result, this method takes a lot of computer power and a big key size. By addressing the key size issue and lowering the computational load for memory optimizing, the suggested combination algorithms approach (AES and ECC) is employed to improve system security in less time.

1.4.2 Limitations

- Even with some significant benefits, there are always disadvantages. For instance, even a genuine user may find it challenging to obtain secured encrypted, legitimate, and electronically signed information at a time when access is important for making decisions.

- Adding cryptographic techniques to the information processing causes a delay, hence cryptography has a value.

- Public-key cryptography usage necessitates the creation and upkeep of public key infrastructure, which is expensive.

- Cryptography cannot be used to guarantee high availability.

1.5 METHODOLOGIES OF PROBLEM-SOLVING

- Generation of Encrypted Data: A hybrid encryption technique will be used to encrypt the confidential data before it is uploaded to the cloud.

- Compression: To make encrypted data smaller so that more information can be concealed using steganography techniques, encryption data will be compressed. The Lempel-Ziv-Welch (LZW) compressing method was utilized in this study and demonstrated success in lowering data size and speed, as seen by the findings in the next section.

- Data concealing in Images: After the image is created, the data hider receives it and has the ability to add extra data to it without getting access to the source image. The data hider just uses LSB replacement to fill all of the accessible bit-planes with more data after determining the number of rows of pixel and bit-planes he can change.

- Calculate Hashing: To ensure that the data is accurate when it is downloaded from the cloud, we will compute the value of the hash of the stego picture in this step. The SHA-256 algorithm was also used in this study to implement integrity. The data owner then stores the stego image in the cloud.

- Checking Hash: Upon downloading the stego-image through the cloud, the data integrity is confirmed by computing its hash and comparing the result with the previously saved hash value.

- Data Extraction with Image Recovery: Here, the LSB technique is used by the receiver to extract the stego-image data, after which it will be feasible to retrieve the merging bits from the cover picture.

- Decompression: The LZW method is used to decompress the data after it has been extracted from the cover picture and returned in its original size.

- Decryption: The hybrid algorithm will be used to decrypt the extracted data in this stage.

Chapter 2: LITERATURE SURVEY

- **PAPER 1:**

  SECURING OF CLOUD DATA WITH DUPLEX DATA ENCRYPTION ALGORITHM

  By combining the RSA, AES algorithm, and a set of rules, the suggested system offers a cryptographic tool for achieving safe information sharing. Design of the cited research: The registered user must upload a file using AES key creation during the uploading phase and encrypt the file's contents using that key. Once the key has been generated, the file is successfully uploaded to the cloud database. The user must ask for a file to be received during the download phase, and the admin checks the user's authentication against the cryptography server it maintains. After it is confirmed, the data is decrypted with a private key and the individual using it is able to successfully download it. 1 Transporting the login screen to the cloud window is a crucial function for the network person. This module was developed with security in mind. Enter your user name and password on this login screen, and it will verify that your information is correct by running a series of security checks. Any incorrect username or password prevents us from entering the login page and causes the window to display an error warning. Therefore, to stop unauthorized individuals from accessing the login window and using the user window. It will assure fact integrity and provide the required facts security for our objective. Since the server already has the user name and password, it also verifies the customer's identity. This will increase security and prevent unauthorized users from accessing the network. Here, it verifies a user's login information and server authentication.

  - **Pros:**

    1. All data transfer records are kept safely with admin.
    2. Checking whether or not the institution of the person and the institution wherein the requested record exists are identical.

  - **Cons:**

    1. Utilizes much more encryption time.
    2. Time taken to decrypt data is also high.

- **PAPER 2:**

  A HYBRID APPROACH FOR ENHANCING SECURITY IN INTERNET OF THINGS (IOT)

  In this research, HAR (Hybrid AES Rail Fence), a hybrid encryption technique, is proposed for safe data transmission between IoT devices. The suggested encryption algorithm preserves confidentiality, making it impossible for attackers to decipher the cypher text, and performs better than traditional encryption techniques. An explanation of a hybrid encryption standard that offers security for many applications, such as transmitting bank OTP notifications to the authorized profile user against getting hacked during the message transfer, is given in this paper. A hybrid algorithm called HAR is put into practise in order to accomplish the aforementioned goal. The hybrid version of the AES Rail Fence encryption method is known as HAR.

  The AES block cypher and Rail Fence transposition cypher are combined in the HAR encryption process to increase security by increasing the difficulty of recovering the original data using various methods including confusion and dispersion. The four processes in the Advanced Encryption Standard (AES) for encrypting plain text are sub bytes, shift rows, mix columns, and add round key. The decryption procedure is represented by these steps in reverse. The result of AES serves as the input to the Rail Fence cypher in the HAR encryption standard, which comes after the process of encryption carried out by AES. A transposition cypher called Rail Fence is a simple and practical approach to zigzag the characters of a word. They utilized the diagonal structure of the pattern that is employed for encryption of the message in the decoding procedure. Generating a grid with the same number of rows as the key and the same number of columns as the cypher text's length is the first step in the procedure.

  - **Pros:**

    1. Dual encryption of the plain text.
    2. Presents a high degree of diffusion.

  - **Cons:**

    1. Performance of system is less-efficient.

- **PAPER 3:**

  SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

  This paper focuses on the use of hybrid cryptosystems to secure cloud computing and cloud storage. In this case, the encryption procedure was carried out in stages. Start by using the file systems module to segment the downloaded file into three sections before encrypting it. Three separate cryptographic methods, including Blowfish (BF), Message Digest (MD5), and AES, are used to encrypt each component. The file that contains the merged sections is then reloaded to the cloud. The decryption phase, in contrast, proceeds in the exact same manner as the encryption phase. Acquire the encrypted file first. It is then divided into three parts that are designated for decoding in accordance with the encryption scheme (Blowfish, MD5, and AES). The blowfish method is applied in this suggested system to store encrypted information in the cloud. Additionally, the blowfish key is encrypted using the EC public key. Blowfish decrypts data using the EC private key's decrypted key. The upload technique uses blowfish encryption, and the download method decodes the blowfish decrypted key.

  - **Pros:**

    1. The message digest tag is utilized to protect the key.
    2. Data protected from side-channel attacks on the cloud.

  - **Cons:**

    1. Low avalanche effect leading to less secure technique.
    2. Power consumption is high.

- **PAPER 4:**

  SECURITY IMPROVEMENT OF CLOUD DATA USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY

  The AES-256 and RSA methods are employed for hybrid encryption in this study, and each RSA and AES are efficient cloud-based encryption techniques. Data that has been encrypted will be condensed to make it smaller and enable steganography to cover up more information. Based on where the secret data is located in the data array, the hybrid encryption divides the data into odd and even data. The AES technique with 256-bit key sizes, generated by a random number generator (RNG), is used to encrypt odd-data. The NIST randomness tests demonstrate that the RNG randomly generates a series of values that cannot be accurately anticipated. While the RSA technique is used to encrypt even-data. where the secure AES key distribution process is employed for encryption. Random number generators (RNGs), that are found within numerous computer software libraries, are used to create the key. b. The RSA technique and a public key are used to encrypt it. c. The key is then securely sent to the other party. Algorithm also mentions hybrid encryption of the secret data. The only information that must be sent when the data proprietor opts for sharing his information with the other party is the encrypted AES key and the stego hash value. The two-security methods encryption and steganography were effectively coupled in this work to offer double protection for data stored in a cloud environment.

  - **Pros:**

    1. Has a higher PSNR value so it becomes harder for visual attackers to recognize the stego-image.
    2. SSIM value of stego-image is closer to 1.
    3. The stego-image generated is of outstanding quality

  - **Cons:**

    1. Size of the key generated is large.
    2. Less number of encryption rounds.

Chapter 3: SOFTWARE REQUIREMENTS SPECIFICATION

3.1 USER CLASSES AND CHARACTERISTICS

- **CHARACTERISTICS**

1. **EXPERIENCE**

   Algorithms that have been used over a long period are less likely to have security flaws than newer algorithms.

2. **PERFORMANCE**

   The time to complete a cryptographic operation is linearly proportional with the input data size.

3. **KEY DISTRIBUTION**

   Keys should be distributed using automatic means.

4. **KEY RE-USE**

   The more times a key is used, the greater the chance of an attacker discovering that key.

5. **MULTI-LAYER SECURITY**

   Using multiple overlapping security mechanisms can increase the security of a system.

3.2 ASSUMPTIONS AND DEPENDENCIES

- **ENCRYPTION**

1. Conventional or cryptography with secret keys are other names for symmetric key cryptography.
2. Asymmetric key cryptography is another name for public key cryptography.
3. In symmetrical key crypto, both encryption (E()) and decryption (D()) use the same private key (K). Two entities, namely KAB, share the secret.
4. Public (PU) and private (PR) keys are used in public key cryptography. A pair of keys are employed, one for encryption and the other for decryption. Every entity has a unique pair, such as (PUA,PRA).
5. Using a key to encrypt unencrypted (or a message), P or M, produces ciphertext C, for example, C = E(KAB,P) or E(PUA,M).
6. With the right key, ciphertext can be decrypted to reveal its original plaintext. The plaintext will be recognised by the decryptor as accurate, indicating that the key is also correct. For instance, P = D(KAB,C) or M = D(PRA,C).
7. The original plaintext cannot be recovered by decrypting ciphertext with the wrong key. The decryptor is going to be able to tell that the key is incorrect because the result of the decryption won't be recognizable.

- **KNOWLEDGE OF ATTACKER**

1. All cryptographic algorithms, such as hash functions and encryption/decryption algorithms, are open to the public.
2. The method being utilised and any of its public parameters are known to an attacker.
3. An attacker can intercept any message sent across a network.
4. Any message sent over a network can be intercepted by an attacker.
5. An attacker is unaware of secret values, such as the private key PRA or the symmetric secret key KAB.
6. It is impossible to carry out brute force attacks that require more than 280 operations.

- **AUTHENTICATION WITH SYMMETRIC KEY AND MACS**

1. Recipient of ciphertext that is successfully decrypted using the symmetric private key KAB is aware that the initial message was not altered and that it came from either A or B, the original holders of the secret key.

2. A recipient of a message with an attached MAC who correctly verifies it understands that the message was not altered and came from one of the MAC secret key owners.

- **HASH FUNCTIONS**

1. The cryptographic hash operation, H(), takes an input message of variable size, M, and generates an output hash of fixed size, h, which is equal to H(M).
2. It is impossible to locate the original message given a hash value, h. M.
3. It is difficult to locate a message M that has the same hash value as a given message h.
4. Finding the two messages, M and M , with the same hash value is impossible.

- **DIGITAL SIGNATURES**

1. A message's digital signature S = E (PR, H(M)) where M is the message's hash encrypted using the signer's private key.
2. A recipient of a communication that has a digital signature attached is aware that the message was signed by the signer.

- **KEY MANAGEMENT AND RANDOM NUMBERS**

1. Private key can be transferred between two separate entities without the value of the key being discovered by other entities.
2. Any entity has access to any other entity's correct public key.
3. Pseudo-random number generators (PRNG) may generate actual random numbers in a useful manner.

3.3. FUNCTIONAL REQUIREMENTS

Table 4: Functional Requirements

ID	Reqiurement
FR01	Every user must be registered with valid ID.
FR02	Every user must have a unique ID for reference.
FR03	The system shall be able to upload different data documents (Text, audio, video files) over cloud securely.
FR04	The system should encrypt the data and create stego image by applying different cryptography and steganography algorithms before storing on cloud.
FR05	The key for decryption and Hash value should be transported at the receiver side.
FR06	The proposed system must authenticate all authorized users to upload or receive data from cloud securely.
FR07	Hash value must be compared and verified at receiver's end for verifying data integrity.
FR08	The system should alert user if the hash value is different as compared to the hash value send by sender.

3.4. EXTERNAL INTERFACE REQUIREMENTS

3.4.1. USER INTERFACES

Any browser, including Internet Explorer, Mozilla, and Netscape Navigator, that a user uses to access the system must be compatible with the user interface of the software. The conversation among a user and a computer is the subject of user interface. From the system's initial startup or login until the final display of required inputs and outputs, it has to do with everything. Dialogue refers to the overall pattern of screens and messages.

3.4.2. HARDWARE INTERFACES

All hardware needed to connect to the internet will serve as the system's hardware interface because the programmed must execute over the internet. For instance, modems, WAN-LANs, and Ethernet Cross-Cables.

3.4.3. SOFTWARE INTERFACES

- The system shall be able to upload different data documents (Text, audio, video files) over cloud securely.
- The suggested system could use various cryptography and steganography techniques to encrypt the data and generate stego images before putting it on the cloud.
- The recipient side should transport the hash value and decryption key.
- The suggested system must securely upload or receive information from the cloud by authenticating each authorized user.
- To ensure the integrity of the data, the value of the hash must be checked and confirmed at the receiver's end.

3.4.4. COMMUNICATIONS INTERFACES

The system shall use the HTTP protocol for communication over the internet and for the intranet communication will be through TCP/IP protocol suite.

3.5. NON-FUNCTIONAL REQUIREMENTS

A non-functional requirement is a requirement that specifies various attributes of a system, rather than specific behaviours. To develop the application, we must consider the following non-functional requirements:

3.5.1. PERFORMANCE

The system should perform its objectives efficiently and effectively as per the requirements. Interactions with the cloud server which require processing, such as login, uploading files and

requesting files and data at receiver end. Over reasonably common internet connection speeds, the cloud server should respond to client requests in less than few seconds.

3.5.2. SECURITY

The system has to be protected. Access to the system is restricted to authorized users only. Each user is verified by providing a valid username and password. To upload or download data and information from the cloud server, users have to be logged in. For security concerns, the system ought to be able to grant users the ability to change their passwords or to reset them if they lose them.

3.5.3. STORAGE

The system ought to leverage cloud storage, where we may store enormous amounts of data—up to 1 Exabyte—for data storage. You can use cloud storage to store files and other information in a remote location that you can access over either an encrypted private network or the open internet.

3.5.4. USER INTERFACE

The system ought to offer a user-friendly "click and go" graphical user interface with buttons, links, and fields. so that the application access failures can be minimized. Common UI components should be present throughout the application. Users feel more at ease and can-do tasks more rapidly when using system UI's common elements.

3.5.5. FLEXIBILITY

Multiple users should be able to use the system (Hardware Device/Application) at a same time from any location. Each request should be processed within few seconds if multiple users are accessing application at a same time. Even in normal internet connectivity the application system should fulfil users request in less time.

3.6. SYSTEM REQUIREMENTS

3.6.1. SOFTWARE REQUIREMENTS

- Operating System: Windows 10
- Language Used: Python

3.6.2. HARDWARE REQUIREMENTS

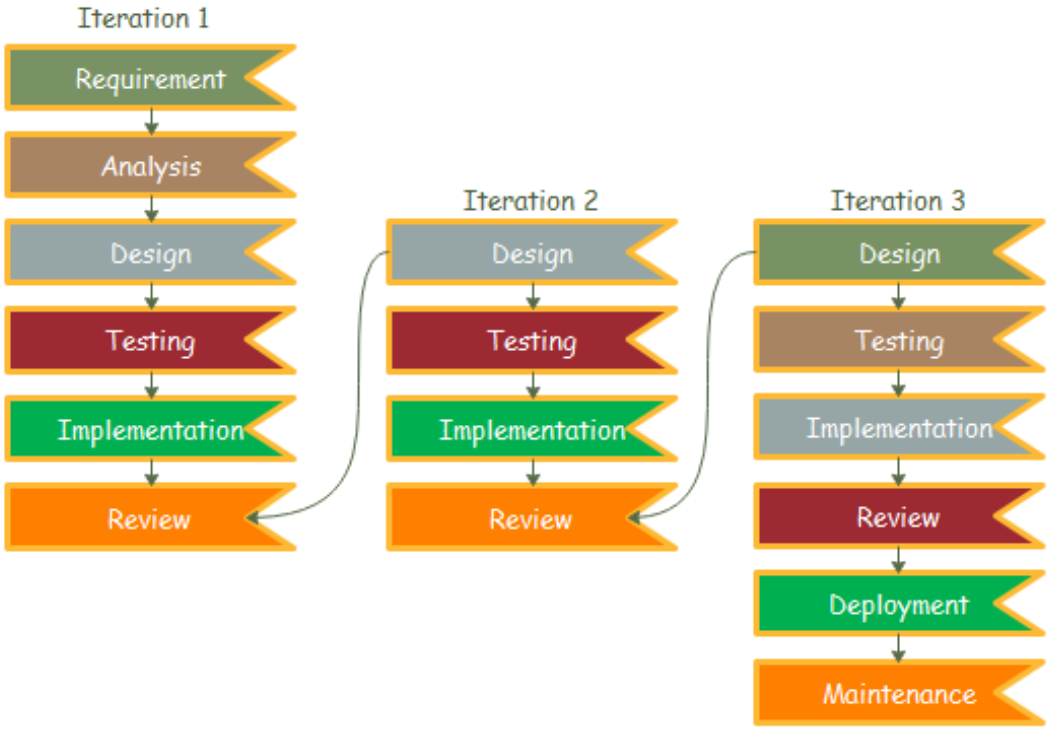
- Processor: Intel CORE i3 or more.
- RAM: Memory of 4 GB RAM or more.

3.7. ANALYSIS MODELS: SDLC MODEL TO BE APPLIED

- **ITERATIVE MODEL**

The iterative procedure represents a software development life cycle (SDLC) approach in which the initial development phase is conducted based on initial requirements that are clearly defined. Iterations are used to add additional features to this base software product until the final system is complete. The objective of this SDLC methodology is not to provide an exhaustive specification plan. The iterative development approach, on the other hand, is a technique for dividing any sizable software development project into smaller pieces. It is intended to build only a section of the program iteratively, starting with the minimal minimum requirements. The prototype is then reviewed once more to see if there are any more requirements, and the remaining planning, requirement analysis, deployment, and maintenance are all carried out. This assists in early risk identification and risk mitigation related to the requirements.

Figure 2: Iterative Model



i. **REQUIREMENTS ANALYSIS**

Potential requirements, deadlines and guidelines for the project are analyzed and placed into a functional specification. This stage handles the defining and planning of the project without mentioning specific processes.

The system specifications are analyzed to generate product models and business logic that will guide production. This is also when financial and technical resources are audited for feasibility.

ii. **DESIGN**

A design specification document is created to outline technical design requirements such as programming language, hardware, data sources, architecture and services.

iii. **CODING/IMPLEMENTATION**

The source code will be developed using the models, logic and requirements designated in the prior stages. Typically, the system is designed in smaller components, or units, before being implemented together.

iv. **TESTING**

This is when quality assurance, unit, system and beta tests take place to report issues that may need to be resolved. This may cause a forced repeat of the coding stage for debugging. If the system passes the tests, the waterfall continues forward.

v. **OPERATION/DEPLOYMENT**

The product or application is deemed fully functional and will be deployed to a live environment.

vi. **MAINTENANCE**

Corrective, adaptive and perfective maintenance will be carried out indefinitely to improve, update and enhance the final product. This could include releasing patch updates or releasing new versions.

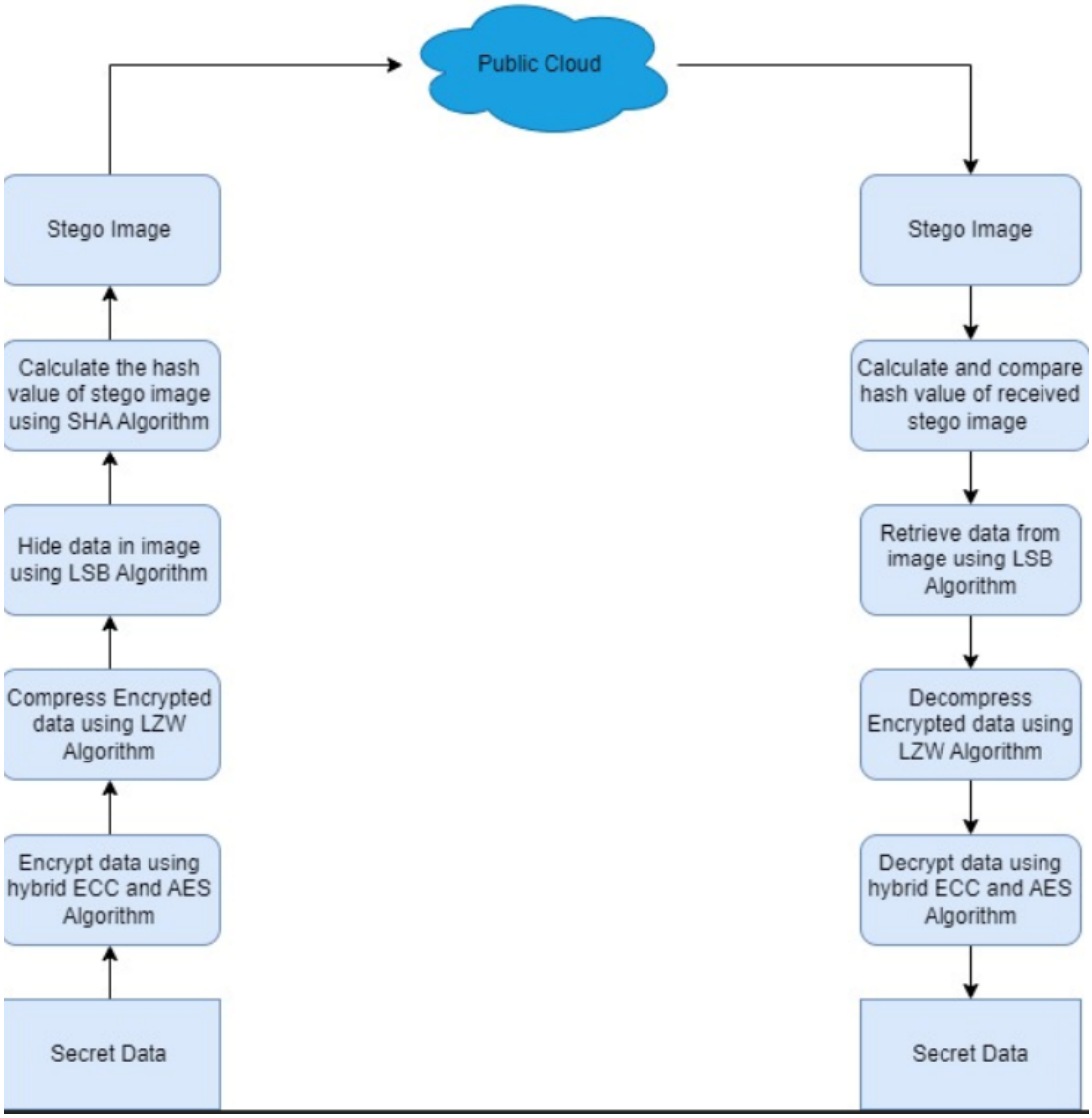
Chapter 4: SYSTEM DESIGN

4.1. SYSTEM ARCHITECTURE AND MODULE DESCRIPTION

4.1.1. SYSTEM ARCHITECTURE

The design of a novel method for providing total security of confidential information in a public cloud model is presented in this section. As an illustration of several cloud kinds, the public cloud has been used. This is so that everyone who wishes to use it can do so. This indicates that the suggested solution is compatible with deployment methodologies for community, private, and hybrid clouds. The following diagram explains the proposed system's architecture flowchart.

Figure 3: System Architecture



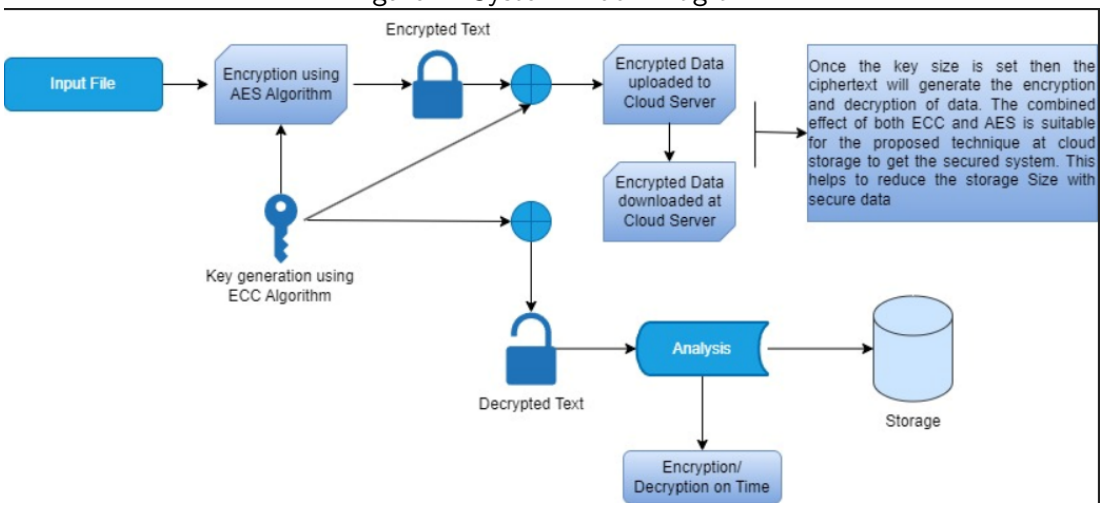
The following processes are included:

- **Encryption:** A hybrid encryption method will be used to encrypt the upload of confidential data to the cloud.
- **Compression:** To make encrypted data smaller so that more information can be concealed using steganography techniques, encrypted data is going to be compressed. The Lempel Ziv-Welch (LZW) reduction technique was utilized in this experiment, and the findings in the next part will demonstrate how well it worked at lowering the data size and speed.
- **Embedding:** Here, we will hide data that has been compressed into a cover image using the Least Significant Bit (LSB) embedding algorithm that will create a stego-image as an output.
- **Calculate Hashing:** In order to verify the data integrity when it is retrieved from the cloud, we will compute the hash value of the stego picture in this phase. The SHA-256 algorithm was also used in this study to implement integrity. The data owner then stores the stego image in the cloud.
- **Checking Hash:** After downloading the stego-image from the cloud, the data integrity is tested by computing the hash value for it and comparing it to the previously stored hash value.
- **Recovery:** In this case, the receiver applies the LSB algorithm to extract the stego-image data, after which it will be feasible to retrieve the merged bits from the cover picture.
- **Decompression:** Following data retrieval from the cover image, decompression software is used to restore the data to its original size.
- **Decryption:** The hybrid algorithm will be used in this stage to decrypt the extracted data. Algorithm 2 is used to implement the hybrid decryption.

4.1.2. SYSTEM BLOCK DIAGRAM

To protect the data kept in the cloud environment, numerous strategies have been proposed and put into practise. Therefore, we have proposed a two-step steganography approach method. The pre-processing algorithm, which shrinks the size of the hidden images, is the first step. As an embedding technique in the second stage, we used an algorithm that depends on the Fibonacci illustration of pixel intensity. The proposed approach, however, does not employ encryption techniques to ensure the secrecy of sensitive data. So, based on encryption and steganography, we developed a hybrid paradigm of data securely stored on the cloud. The ECC, AES, and LSB algorithms are used to encrypt sensitive data, which is then concealed via LSB prior to publishing to the cloud. In order to increase the security of cloud storage, we have also used the SHA-256 hash method to verify integrity. According to their findings, an excellent PSNR value might be attained to disguise 1KB of data as a picture.

Figure 4: System Block Diagram



4.2. DATA FLOW DIAGRAMS

The classic visual representation of how information moves through a system is a data flow diagram (DFD). A tidy and understandable DFD can graphically represent the appropriate quantity of the system demand. It can be done manually, automatically, or both. It demonstrates how information enters and exits the system, what modifies the data, and where information is kept. A DFD's goal is to outline the boundaries and scope of the structure as a whole. It can be utilised as a communication tool among a system analyst and any participant in the sequence that serves as the foundation for system redesign. The DFD is also known as a bubble chart or data flow graph.

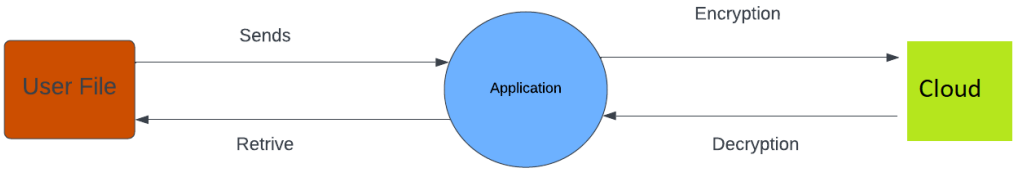
- **LEVELS IN DATA FLOW DIAGRAMS (DFD)**

  Any level of abstractions for a system or piece of software can be performed using the DFD. In reality, DFDs can be divided into stages that signify a growth in flow of information and functional granularity. In DFD, levels are denoted by the numbers 0, 1, or 2. The data flow diagram in this example has three main levels: 0-level DFD, 1-level DFD, and 2-level DFD.

1. **0-LEVEL DFD**

   Figure 1 displays the Level-0 DFD, also known as the context chart of the result system for management. The associated data flow may also need to be divided as the bubbles are broken down into ever-less abstract bubbles.

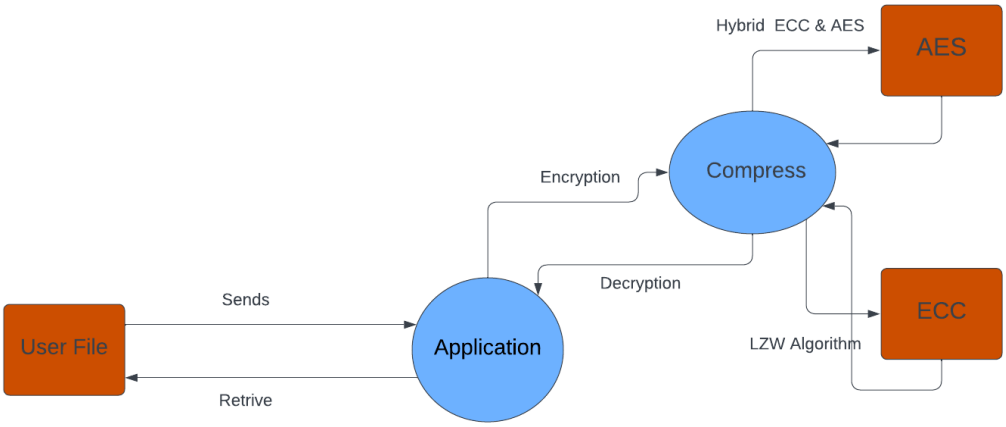
Figure 5: DFD Level 0



2. **1-LEVEL DFD**

   A context diagram is divided into various bubbles and processes in 1-level DFD. At this stage, we draw attention to the system's primary goals and deconstruct the high-level DFD process into its component parts.

Figure 6: DFD Level 1



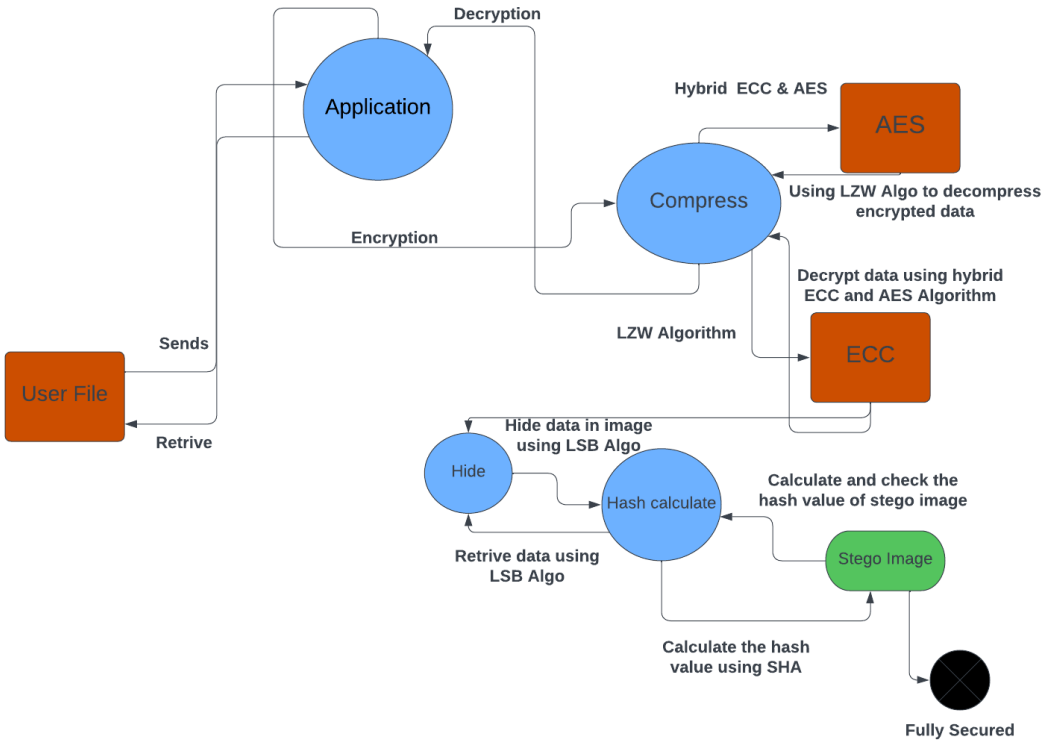
3. **2-LEVEL DFD**

   Components of 1-level DFD are further processed in 2-level DFD. It can be utilized to project or document the precise/important information about how the system operates.

4.3. UML DIAGRAMS

In order to better understand, update, maintain, or document information about the system, a UML diagram is a schematic based on the UML (Unified Modelling Language) that aims to visually describe a system together with its primary players, roles, actions, artefacts, or classes. The primary goal of UML is to establish a uniform method for visualising a system's design process. It resembles plans used in other engineering disciplines quite a bit. UML is a visual language rather than a programming language. To depict the behaviour and framework of a system, we use UML diagrams.

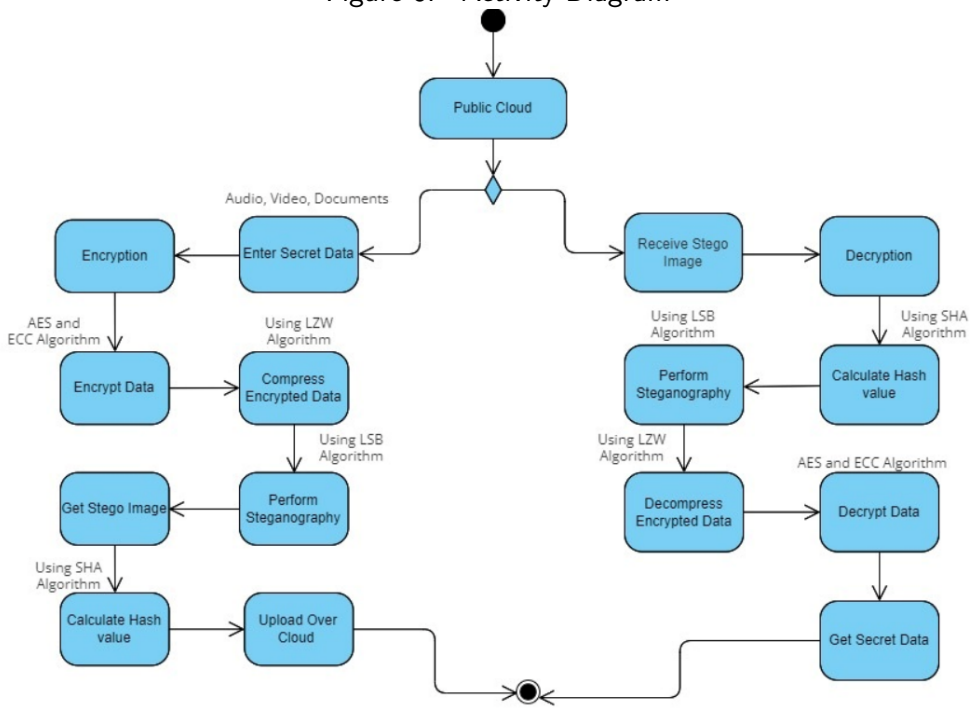
Figure 7: DFD Level 2



4.3.1. ACTIVITY DIAGRAM

Activity diagrams show how multiple levels of abstraction of operations are coordinated to produce a service. Typically, an event must be accomplished by some operations, especially when the operation is meant to accomplish several different things that call for coordination. Another common requirement is how the occurrences in a single use case relate to one another, especially in use cases where operations may overlap and require coordination. It is also appropriate for illustrating how a set of coordinated use cases represents business workflows.

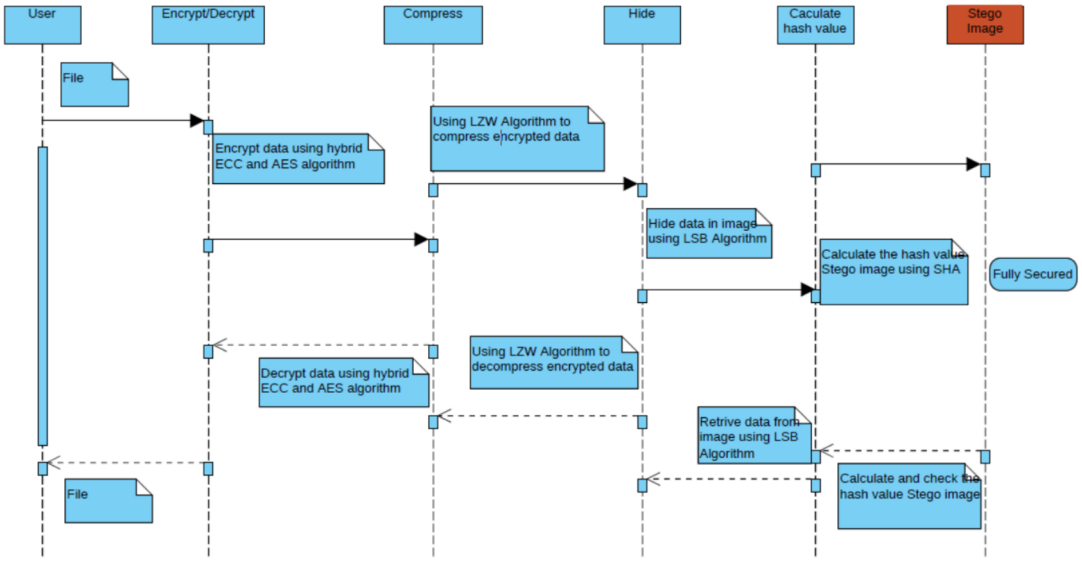
Figure 8: Activity Diagram



4.3.2. SEQUENCE DIAGRAM

A sequence diagram is a diagram created using the Unified Modelling Language (UML) that shows the flow of messages sent and received by objects during an interaction. A set of things that are portrayed by lifelines and the messages they exchange over the course of an interaction make up a sequence diagram. The order in which messages are transferred between objects is depicted in a sequence diagram. Sequence diagrams can also display the command chains that link items. The objects and the communications exchanged between them are depicted in the sequence diagram.

Figure 9: Sequence Diagram



4.3.3. USE CASE DIAGRAM

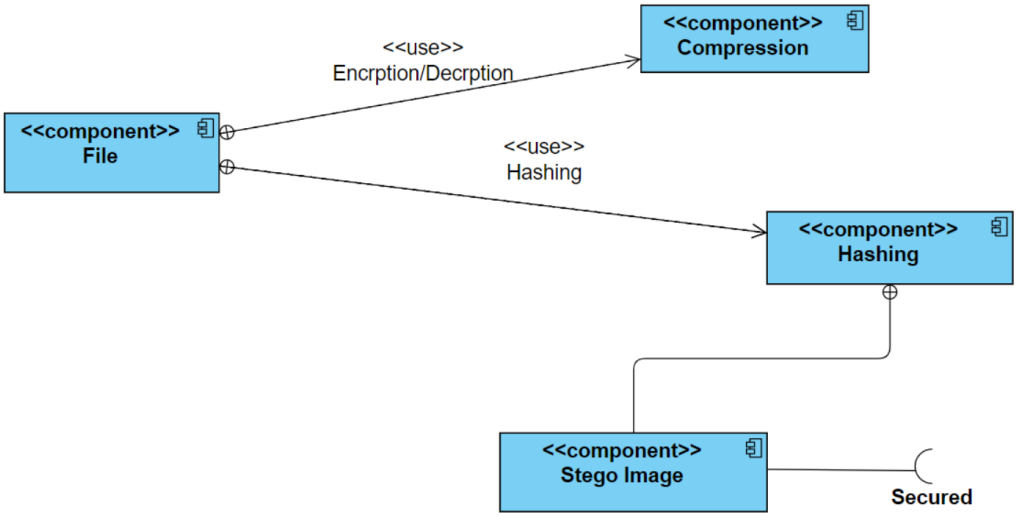
A graphical representation of a user's likely interactions with the system is called a use case diagram. A use case diagram, which is frequently complemented by other types of diagrams, displays the numerous use cases and user types the system has. Either circles or ellipses are used to depict the use cases. The scope and high-level functions of a system are described in use-case diagrams. The connections between the system and its actors are also depicted in these diagrams. utilise-case diagrams show what the structure does and the way the actors utilise it, but they do not show how the system works within.

Figure 10: Use Case Diagram

4.3.4 COMPONENT DIAGRAM

A UML component diagram provides a top-down perspective of your software system. You will become a better developer if you comprehend the precise service behaviour that each component of your product delivers. Software systems that are built with any programming language or fashion can be described using component diagrams. There are many different applications for the set of rules known as UML for object-oriented diagrams. The Unified Modelling Language requires that components and packages be wired together in component diagrams using lines that represent assembly connectors and delegate connectors.

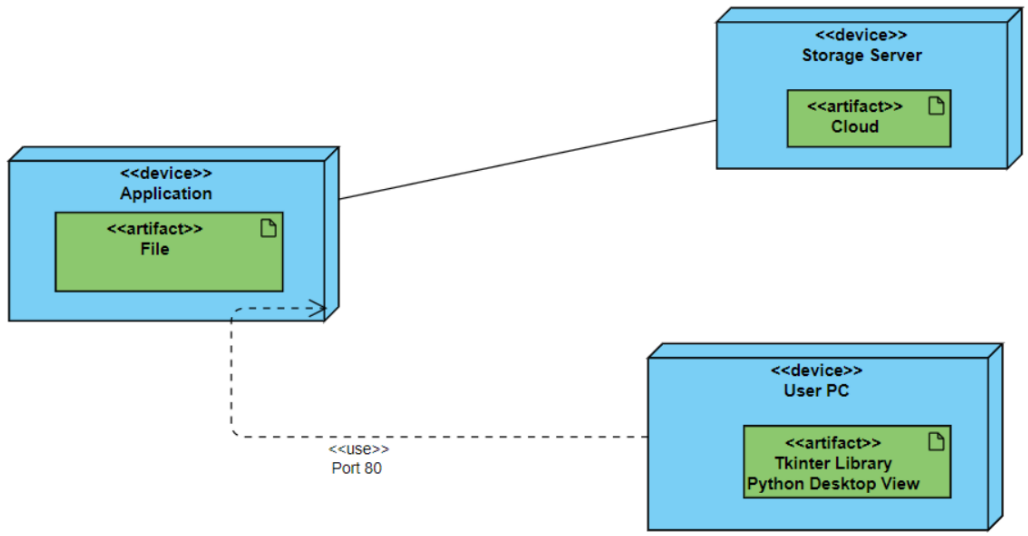
Figure 11: Component Diagram



4.3.5 DEPLOYMENT DIAGRAM

Deployment diagrams in UML represent a system's physical architecture. The relationships between the system's hardware and software components as well as the actual placement of the processing are displayed in deployment diagrams. The physical configuration of a distributed system's nodes, the artefacts that are stored on each node, and the elements and other aspects that the artefacts implement are all displayed on deployment diagrams, which you normally create during the implementation phase of development. Nodes represent hardware components like computers, sensors, printers, and other components that support a system's runtime environment. The links in the system are modelled by communication routes and deploy relationships.

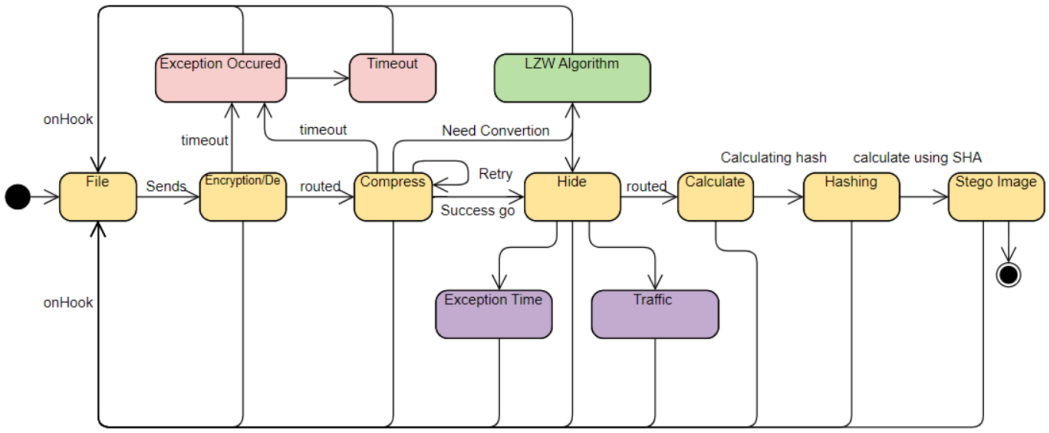
Figure 12: Deployment Diagram



4.3.6 STATE DIAGRAM

A state diagram in the Unified Modelling Language (UML) depicts the stages an object can reach as well as the transitions among those states. It is also referred to as a diagram of a state machine or state chart diagram. A state, which in this case refers to a particular entity in the programme or the unit of code that represents that thing, describes a stage in the development or behaviour of an object.

Figure 13: State Diagram



Chapter 5: PROJECT PLAN

5.1. PROJECT ESTIMATE

5.1.1 Reconciled Estimates

- Cost Estimate

  Cost of project:

  C=N*Cp

  C=4*5000

  C=20,000

  The Cost of the project is approximately up to 20000.

- Time Estimate

  Line of Code (LoC): The average estimation of this project is 15000 to 18000 lines of code.

- LOC based Estimation

  Efforts in Person in months E = 3.2 (KLOC)1.05 E = 3.2 (9.01.05to11.0) 4.21.05

Table 5: LOC-Based Estimation

Function	**Estimated KLOC**
GUI design	1.1-1.3
Logical code	1.5-2.0
Location Based code	1.1-1.3
Directory matching code	1.0-1.3
Business logic	2.2-2.5
Testing	1.1-1.2
Re-correction of Code	1.0-1.2
Total	< 9.0-10.11

Utilization per man month the following sub activities make up the man-month estimate:

- The team member's technical training will take close to a month. Included in this are Java, JSP, etc.
- Research: Given that the initiative is original, research is crucial and currently appears to take one to one and a half months.

5.1.2. Project Resources

1. **Software Requirements**
   - Operating System: Windows 10
   - Language Used: Java, JSP, MySQL
2. **Hardware Requirements**
   - RAM: Memory of 4 GB RAM or more
   - Processor: Intel CORE i3 or more.

5.2. RISK MANAGEMENT

5.2.1 Risk identification

A study of the project scope, objectives specifications, and schedule for the project are done for risk identification.

1. Have top software and customer managers formally committed to support the project

   Ans: All the required software's for developing the system is freely available and hence development will be possible.

2. Are end-users enthusiastically committed to the project and the system/product to be built?

   Ans: Yes. The end user will use this system to secure their data and information.

3. Are requirements fully understood by the software engineering team and its customers?

   Ans: Yes. All the requirements are fully understood by our team.

4. Do end-users have realistic expectations?

   Ans: Yes

5. Does the software engineering team have the right mix of skills?

   Ans: Yes, we have.

6. Are project requirements stable?

   Ans: All the basic requirements for this project are stable, although some are variable but can be fulfilled.

7. Is the number of people on the project team adequate to do the job?

   Ans: Yes.

8. Do all customer/user constituencies agree on the importance of the project and on the requirements for the system/product to be built?

Ans: Yes.

5.2.2 Risk Analysis

The risks for the Project can be analyzed within the constraints of time and quality:

Table 6: Risk Table

ID	Risk Description	Probability	Impact		
			Schedule	Quality	Overall
1	Deadline Risk	Medium	Low	Medium	Medium
2	Technical Skill Risk	Medium	Low	Medium	Medium
3	Hardware Failure Risk	Low	Low	Low	Low
4	Accuracy Risk	Medium	Medium	Medium	Medium

Table 7: Risk Probability Definitions

Probability	Value	Description
High	Probability of occurrence is	$< 25\%$
Medium	Probability of occurrence is	$> 75\%$
Low	Probability of occurrence is	$< 25\%$

Table 8: Risk Impact Definitions

Impact	Value	Description
Very High	> 10 %	Schedule impact or Unacceptable quality
High	$< 10\%$ is	Schedule impact or Some parts of the project have low quality
Medium	$> 15\%$	Schedule impact or Barely noticeable degradation in quality Low Impact on schedule or Quality can be incorporated

5.2.3 Overview of Risk Mitigation, Monitoring, and Management

Table 9: Risk 1

Risk ID	1
Risk Description	Development Deadline Risk
Category	Development Environment
Source	Software requirement Specification document
Probability	Medium
Impact	High
Response	Mitigate
Strategy	Team Work distribution and Task plan
Risk Status	Identified

Table 10: Risk 2

Risk ID	2
Risk Description	Proper Integration of Modules to create hybrid module
Category	Development Environment
Source	Requirements
Probability	Low
Impact	High
Response	Mitigate
Strategy	Proper analysis of algorithms
Risk Status	Identified

Table 11: Risk 3

Risk ID	3
Risk Description	Fetch data from the cloud
Category	Requirements
Source	Software requirement Specification document
Probability	Low
Impact	High
Response	Mitigate
Strategy	Proper connection to the cloud.
Risk Status	Identified

5.3 Project Schedule

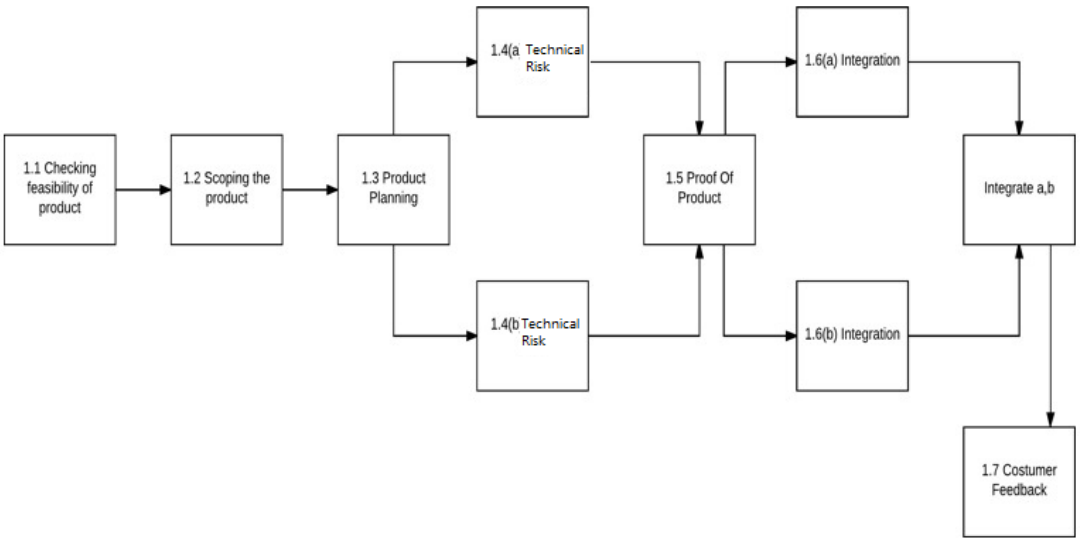
5.3.1 Project Task Set

Major Tasks in the project stage are:

- Task 1: Checking the Feasibility of the Product.
- Task 2: Scope of Product.
- Task 3: Product Planning.
- Task 4: Checking Technical Risk.
- Task 5:Implementation of AES and ECC algorithms.
- Task 6: Implementation of hybrid cryptographic algorithm.
- Task 7: Setting up a cloud.
- Task 8:Connecting the cloud.
- Task 9: Performing the system analysis.
- Task 10: End user feedback.

5.3.2 Task Network

Figure 14: Task Network



5.3.3 Timeline Chart

Figure 15: Gantt Chart SEM 1

Task	Start Date	End Date	Duration
Domain Selection	25-07-2022	05-08-2022	11
Guide Allocation and Idea gathering	06-08-2022	12-08-2022	6
Idea discussion and Abstract submission	12-08-2022	25-08-2022	13
Project Review 1	30-08-2022	01-09-2022	2
Submission of Final proposal	01-09-2022	12-09-2022	10
Literature Survey	10-09-2022	15-09-2022	5
Domain scope	12-09-2022	16-09-2022	4
Requirement Analysis	16-09-2022	20-09-2022	4
Features and Objectives	17-09-2022	22-09-2022	5
System Design and Architecture	23-09-2022	15-10-2022	22
Project Review 2	21-10-2022	21-10-2022	2
Report Writing and Final Report Submission	21-10-2022	14-11-2022	24
Project Stage 1 Oral	23-11-2022	24-11-2022	2

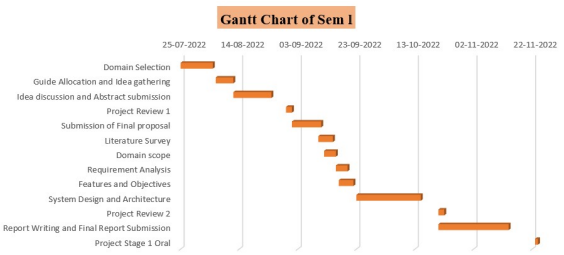
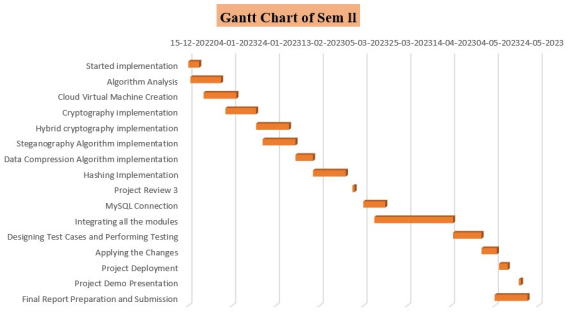


Figure 16: Gantt Chart SEM 2

Task	Start Date	End Date	Duration
Started implementation	15-12-2022	20-12-2022	5
Algorithm Analysis	16-12-2022	30-12-2022	14
Cloud Virtual Machine Creation	22-12-2022	06-01-2023	15
Cryptography implementation	01-01-2023	15-01-2023	14
Hybrid cryptography implementation	15-01-2023	30-01-2023	15
Steganography Algorithm implementation	18-01-2023	02-02-2023	15
Data Compression Algorithm implementation	02-02-2023	10-02-2023	8
Hashing Implementation	10-02-2023	25-02-2023	15
Project Review 3	28-02-2023	28-02-2023	1
MySQL Connection	05-03-2023	15-03-2023	10
Integrating all the modules	10-03-2023	15-04-2023	36
Designing Test Cases and Performing Testing	15-04-2023	28-04-2023	13
Applying the Changes	28-04-2023	05-05-2023	7
Project Deployment	06-05-2023	10-05-2023	4
Project Demo Presentation	15-05-2023	15-05-2023	1
Final Report Preparation and Submission	04-05-2023	19-05-2023	15



5.4 Team Organization

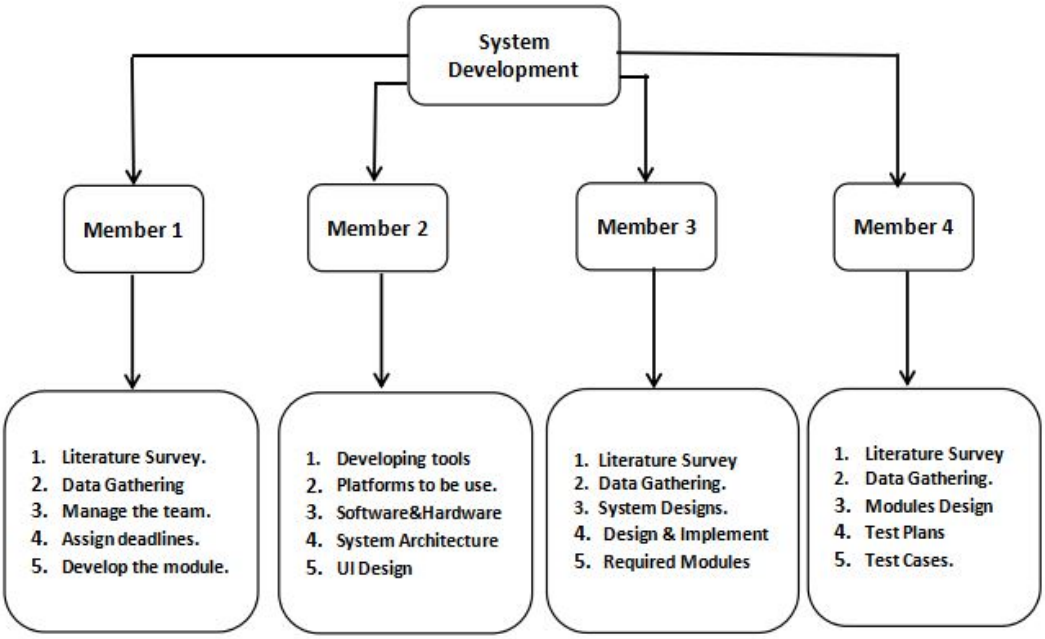
Team Members Details:

1. **Member 1:** Ayush Bolla (Team Leader).
2. **Member 2:** Deep Pawar.
3. **Member 3:** Pranit Rathod.
4. **Member 4:** Vishakha Matkar .

5.4.1 Team Structure

The team structure for the project is identified and roles are defined. Our team has four members. All the members performed the following tasks which are assigned to them.

Figure 17: Team Work Distribution



5.4.2 Management Reporting and Communication

Table 12: Reporting

Sr. No.	Reporting Date	Project Activity
1	13 Jan 2023	Domain Selection
2	13 Jan 2023	Guide allocation and Idea gathering
3	13 Jan 2023	Idea discussion and Abstract submission
4	13 Jan 2023	Done literature survey
5	13 Jan 2023	Requirement Analysis
6	13 Jan 2023	Identified and discussed features, functionalities, and objectives of the selected problem statement
7	13 Jan 2023	System Design and Architecture
8	13 Jan 2023	Report Writing and Report Submission
9	13 Jan 2023	Gathered all the requirements for the project
10	13 Jan 2023	Study and analyzed all the selected algorithms for encryption and decryption
11	13 Jan 2023	Started implementation of AES (Advanced Encryption Standard) algorithm for encrypting the private data
12	13 Jan 2023	Started implementation of ECC (Elliptic Curve Cryptography) algorithm for encrypting and decryption of private data.
13	13 Jan 2023	Identified the way to combine both the AES and ECC algorithm for creating hybrid encryption and decryption model.
14	13 Jan 2023	Remaining Modules Implementation
15	13 Jan 2023	Performed Test Cases and Quality Assurance
16	13 Jan 2023	Final Project Demo and Report Submission

CHAPTER 6: PROJECT IMPLEMENTATION

6.1 OVERVIEW OF PROJECT MODULES

In this system, a fresh approach to safeguarding data kept in the cloud is put forth by fusing the methods of steganography and cryptography modules. In this, the symmetrical encryption technique AES256 and asymmetric encryption method ECC are used to hybridly encrypt confidential data. The encrypted data is then transmitted to the LSB algorithm for concealment after being compressed. Hash functions are employed to swiftly verify the data's objectivity following retrieval.

6.2 TOOLS AND TECHNOLOGIES USED

6.2.1 Java

A wide range of software applications can be made using the highly well-liked programming language known as Java. It's an object-oriented language that's easy to read, write, and comprehend. Java runs on a variety of operating systems, including Windows, Mac, Linux, and Raspberry Pi. It is among the most widely used programming languages worldwide. In the current work market, there is a high need for it. It is simple to use and simple to learn. It is both free and open-source. Java is an object-oriented language that provides programmers with a clear structure and enables code reuse, reducing development costs. Java is similar to C++ and C#, so programmers can easily transfer from one to the other.

6.2.2 JSP

The abilities of the Web server are increased by Java programs known as Java servlets or Java server pages (JSPs), which operate on a Java application server. Java servlets are Java classes created with the specific purpose of responding to HTTP requests within a Web application. You can think of JSPs as an extension of HTML that enables you to smoothly incorporate Java code snippets into your HTML pages. These Java script snippets produce dynamic content that is integrated with the other HTML/XML information. On the server, a JSP is converted into a Java servlet and run. The servlet produced from the JSP contains JSP statements that were embedded in the JSP. On the server, the generated servlet is run.

6.2.3 MySQL

A database management system is MySQL. A systematic collection of data is called a database. It might be anything, such as a straightforward grocery list, a photo gallery, or the enormous amount of data in a business network. A database management system, such as MySQL Server, is required to add, utilization, and process data contained in a computer database. Database management systems, whether used as stand-alone programmes or as a component of other programmes, are essential to computing because computers are excellent at processing

vast volumes of data. Relational databases include MySQL. Instead of placing all the data in one huge warehouse, a relational database keeps the data in individual tables. Physical files that are optimized for speed contain the database structures.

6.2.4 SWING

Swing is a Java Foundation Classes [JFC] library and an extension of the Abstract Window Toolkit [AWT]. Swing offers much-improved functionality over AWT, new components, expanded components features, and excellent event handling with drag-and-drop support. Swing is a Set Of API (API- Set Of Classes and Interfaces). Swing is Provided to Design Graphical User Interfaces. Swing is an Extension library to the AWT (Abstract Window Toolkit). Includes New and improved Components that have been enhancing the looks and Functionality of GUIs'.

6.3 ALGORITHM DETAILS

6.3.1 Encryption and Decryption using AES algorithm

AES is an ongoing cypher as opposed to a Feistel one. Its foundation is a "substitution-permutation network." It consists of a number of interconnected processes, some of which require swapping inputs for particular outputs (substitutions), while others involve randomising bits (permutations). It's interesting to note that AES uses bytes instead of bits for all of its calculations. As a result, AES considers a plaintext block's 128 bits to be 16 bytes. For processing as a matrix, these 16 bytes are set up in four columns plus four rows. In contrast to DES, the number of rounds in AES varies and is based on the size of the key. For 128-bit keys, AES employs 10 rounds; for 192-bit keys, 12 rounds; and for 256-bit keys, 14 rounds. These rounds each employ a distinct 128-bit round key.

6.3.2 Data compression using LZW algorithm

Abraham Lempel, Jacob Ziv, and Terry Welch developed the table-based lookup technique known as LZW compression to compress a file into a smaller file. A specific LZW compression technique makes an entry in a table (also termed a "dictionary" or "codebook") for each input sequence of bits of a defined length (for instance, 12 bits), which includes the pattern itself and a shorter code. Reading a series of symbols, stringing them together into strings, and then translating the strings into codes is how LZW compression operates. We obtain compression because the codes consume less space that the strings they replace.

6.3.3 LSB IMAGE STEGANOGRAPHY SYSTEM

Least Significant Bit is what it means. The rationale underlying LSB integration is that there won't be a significant change in the color if we change the final bit value of a pixel. For illustration, 0 is black. Since it is still black, it won't significantly change if the value is changed to 1. It will merely be a lighter shade of black.

6.3.4 HASHING USING SHA-256 ALGORITHM

Any key or string of characters can be transformed into another value by hashing. The original string is typically represented with a shorter, fixed-length value or key that makes it simpler to locate or use. Implementing hash tables is the most well-liked application of hashing. Key and value pairs are kept in a list that can be accessed by a hash table's index. The hash function will associate the keys to the size of the table because the combinations of keys and values are infinite. The index for a given element is then changed to a hash value.

CHAPTER 7: SOFTWARE TESTING

7.1 TYPE OF TESTING

1. **Unit Testing:** To assure the quality of each component, each one is tested individually. The goal is to find design and implementation flaws.
2. **Integration Testing:** To assure the quality of the resulting unit, a set of dependent components is evaluated collectively. Utilising a progressive integration strategy, the "big bang" problem is avoided.
3. **System Testing:** The software for the system is tested in its entirety. In order to ensure that it functions properly under severe load and that the system doesn't crash, we tested entire modules one at a time.
4. **Validation Testing:** Various fields, including a valid username, a mobile number, and many more, were subjected to validation testing. Each field has been correctly checked and is undergoing testing.
5. **GUI Testing:** We carried out GUI testing on each module to ensure that it functions as expected and that the GUI is appropriately integrated into all the pages.

7.2 TEST CASES & TEST RESULTS

Table 13: Test Cases

TC_ID	Test Case Description	Test Case Steps	Expected Result	Actual Result	Status
TC_1	To check whether admin can log in to the system or not.	1. Run the project 2. Enter UserID and Password 3. Click on login.	It should log in successfully	It is logged in successfully	Pass
TC_2	To check whether New User can register or not.	1. Run the project 2. Click on New User tab. 3. Enter the details.	It should create new user.	It creates the new user.	Pass
TC_3	To check whether whether	1. Log in to the system.	It should fetch the data	It is fetches the data	Pass

TC_ID	Test Case Description	Test Case Steps	Expected Result	Actual Result	Status
	it can browse the data to be encrypted.	2. Click on browse 3. Select the data to be encrypted.	to be encrypted.	successfully.	
TC_4	To check whether it loads the image after loading in to the system	1. Click on browse 2. Select the image 3. Click on Open and Load.	It should load the image.	It loads the image successfully	Pass
TC_5	To check whether it can generate the key or not.	1. Load the image. 2. Click on Generate Key.	It should generate the secret key.	It generates the secret key	Pass
TC_6	To check whether data gets encrypt or not.	1. Load the image. 2. Generate the Key. 3. Click on "Encrypt" to encrypt the data.	It should encrypt the data.	Data is encrypted	Pass
TC_7	To check whether the key hides in the image or not.	1. Encrypt the data by clicking on "Encrypt" tab. 2. Click on "Hiding Key generator to to hide the key	It should hide the secret key.	Key is successfully hidden	Pass
TC_8	To check whether the encrypted data gets sent to the receiver or not.	1. Encrypt the data and hide the key. 2. Click on "Send" 3. Enter receiver's data and click on "Send"	It should send the encrypted data to the receiver.	Data is sent to the receiver	Pass
TC_9	To check whether the receiver can access. the encrypted. data or not.	1. Login as receiver. 2. Click on Image and Message. Extraction Tab.	It should give the decrypted data to the receiver.	Receiver received decrypted data	Pass
TC_10	To check whether user can log out.	1. Click on username. 2. Select Log Out	It should log out.	User is logged out from the system.	Pass

CHAPTER 8: RESULTS

8.1 OUTCOMES

In order to ensure confidentiality and boost security in internet communications, a hybrid cryptography method is created. The following results were attained as a result of this project's implementation:

1. **Hybrid Encryption:**

   A cryptographic technique known as hybrid encryption combines the advantages of both asymmetric and symmetric encryption techniques. Modern secure communication systems frequently use it because it strikes a balance between efficiency and security. A random symmetric key for encryption is created for each communication or session in hybrid encryption. With the help of a quick and effective symmetric encryption method like AES (Advanced Encryption Standard), this symmetric key is utilised to encode the real communication. Because it acts on blocks of data and is typically faster than asymmetric encryption, symmetric encryption is effective. The person receiving it uses their private key to decrypt the symmetric key after getting the message and encrypted version of it.

2. **Secure Stored Data in The Cloud:**

   Securing stored data in the cloud involves employing techniques such as steganography (stego) and cryptography.

   - Cryptography: Cryptography involves the use of mathematical algorithms to convert plaintext data into ciphertext, making it unreadable to unauthorized individuals. It ensures confidentiality and integrity of the data. When securing data in the cloud, the following cryptographic techniques can be applied:
   - Encryption: Encrypting the data before storing it in the cloud ensures that even if an unauthorized party gains access to the data, they won't be able to understand its content.
   - Hashing: Hash functions generate a fixed-size unique value (hash) based on the input data. Hashing can be used to verify the integrity of stored data. Any changes to the data will result in a different hash value, indicating tampering.
   - Steganography: Involves hiding data within other innocuous-looking data to conceal its existence. In the context of securing stored data in the cloud, steganography can be used in conjunction with cryptography to provide an extra layer of protection.

3. **Stego-image quality after hiding:** The quality of a stego-image, which is an image that has been used to hide secret data using steganography, depends on several factors. The primary goal of steganography is to ensure that the hidden data remains undetectable while

minimizing any visible changes to the carrier image. Here are a few considerations related to stego-image quality:

- Imperceptibility: The most important aspect is that the alterations made to the carrier image should be imperceptible to the human eye. The changes introduced by hiding the data using the LSB algorithm should be subtle enough so that the stego-image appears visually similar to the original, unaltered image. If the modifications are noticeable, it may raise suspicion and potentially lead to the discovery of the hidden data
- Visual Quality: The steganography technique used should aim to preserve the visual quality of the image. The human visual system is highly sensitive to changes in certain image characteristics, such as sharpness, color distribution, and texture. Therefore, it is essential to select steganography algorithms and parameters that minimize any degradation in image quality.

4. **Double Security:** Combining cryptography and steganography can indeed provide an additional layer of security for stored data in the cloud environment. By using both techniques together, you can benefit from the strengths of each approach. Here's how you can leverage cryptography and steganography for double security
   - Cryptography: Implement strong encryption algorithms to protect the confidentiality and integrity of the data. This involves encrypting the data using symmetric or asymmetric encryption techniques.
   - Encryption: Encrypt the sensitive data using a robust encryption algorithm like AES (Advanced Encryption Standard). This ensures that even if the data is accessed or intercepted, it remains unreadable and confidential.
   - Steganography: Apply steganography techniques to hide the encrypted data within other files or media, making it harder for unauthorized individuals to detect the presence of sensitive information.
   - LSB Algorithm: Utilize the Least Significant Bit (LSB) algorithm in steganography to embed the encrypted data within the carrier files. By altering the least significant bits of the carrier file's data, the hidden information can be concealed.

8.2 SCREENSHOTS

Figure 18: Register Page

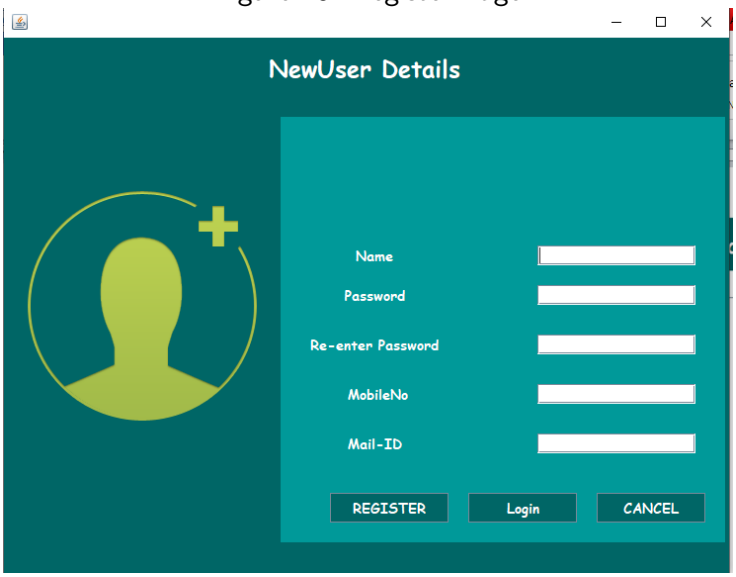


Figure 19: Login Page

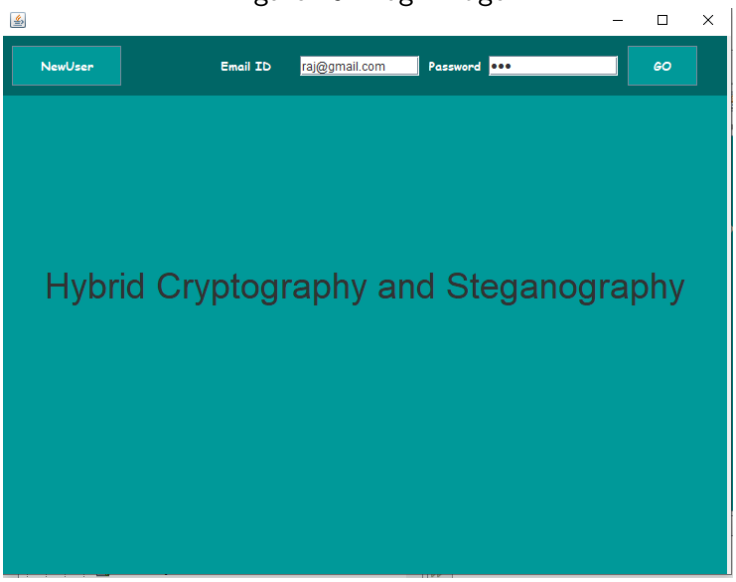


Figure 20: Home Page

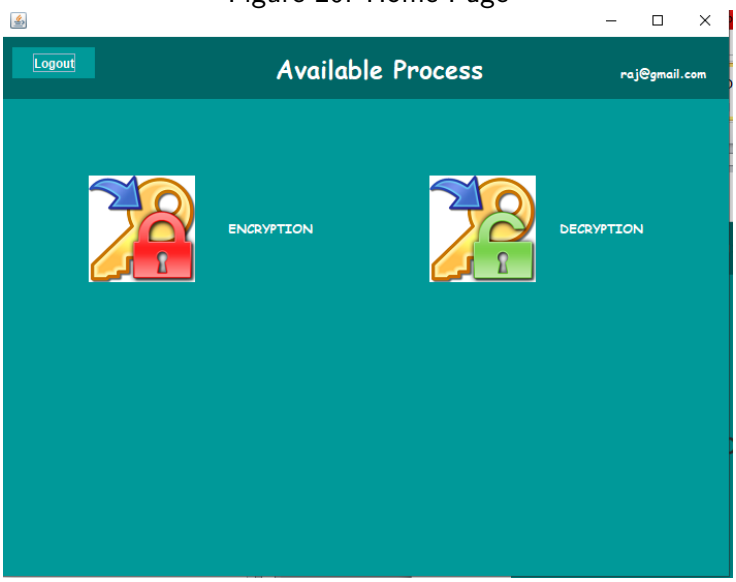


Figure 21: File Upload

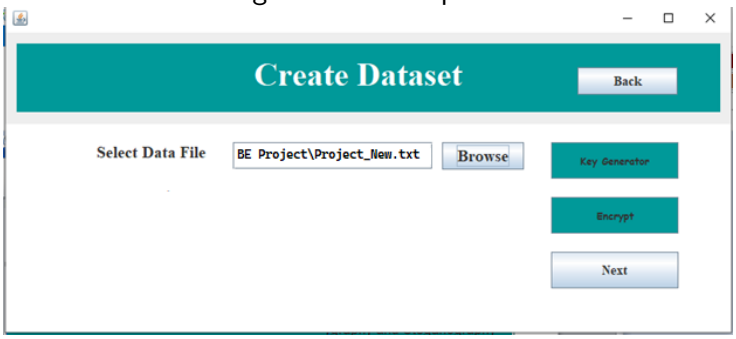


Figure 22: Key Generation

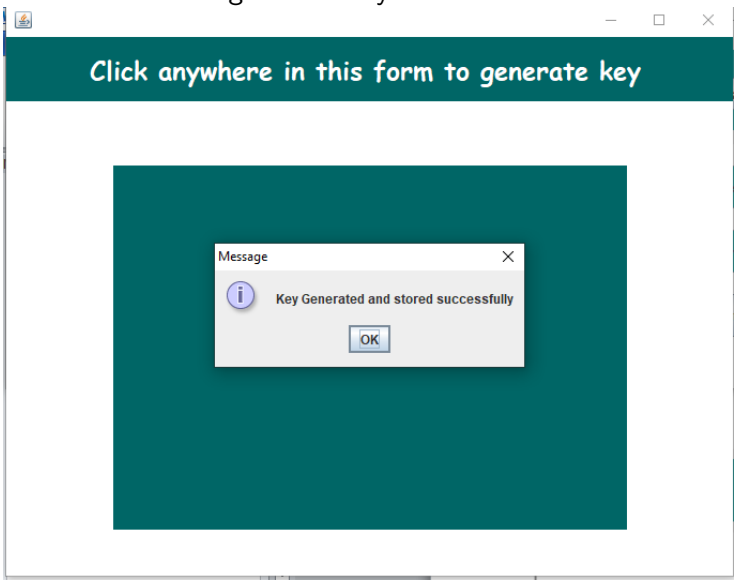


Figure 23: File Encryption

Figure 24: Image Upload

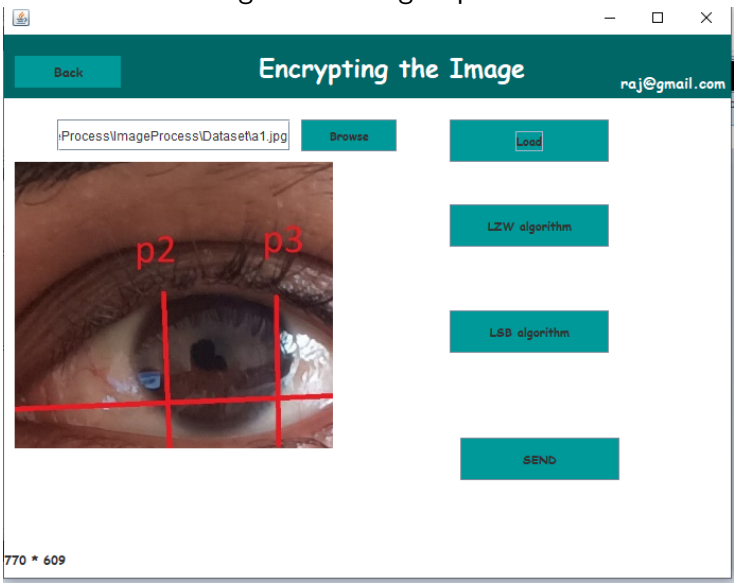


Figure 25: Embedded Image

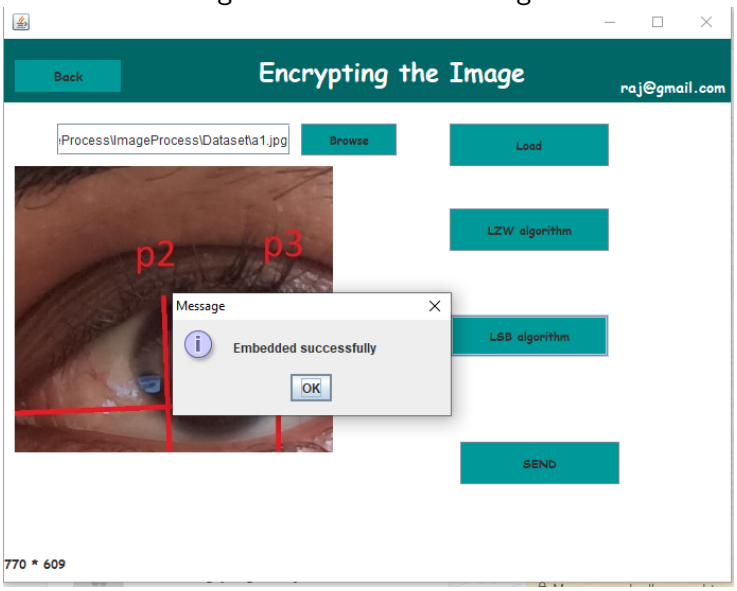


Figure 26: Send Image

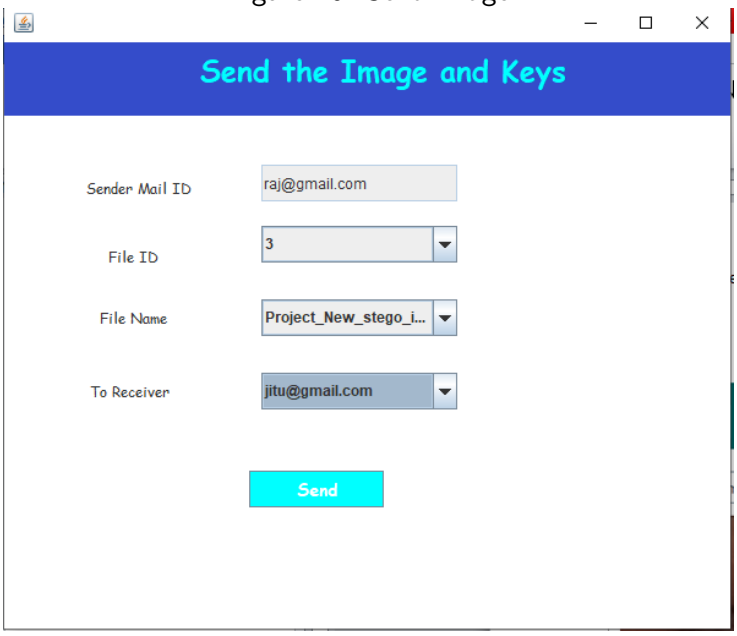


Figure 27: Show Image Data

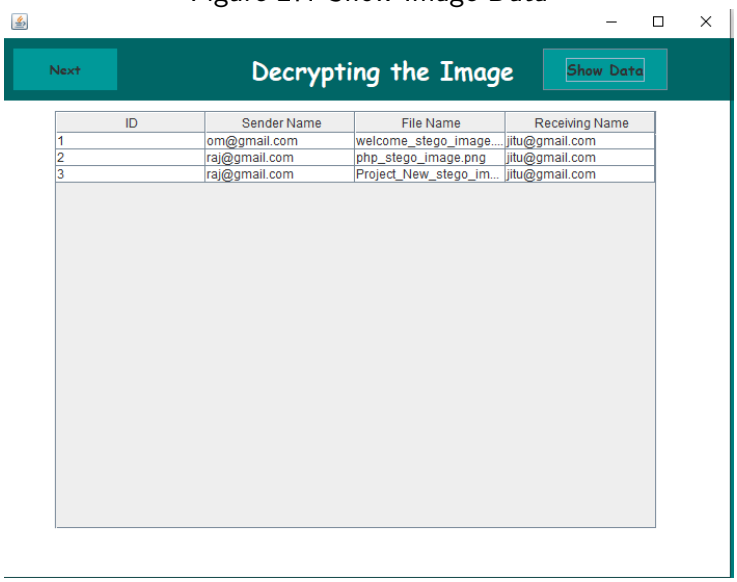


Figure 28: Upload Stego Image

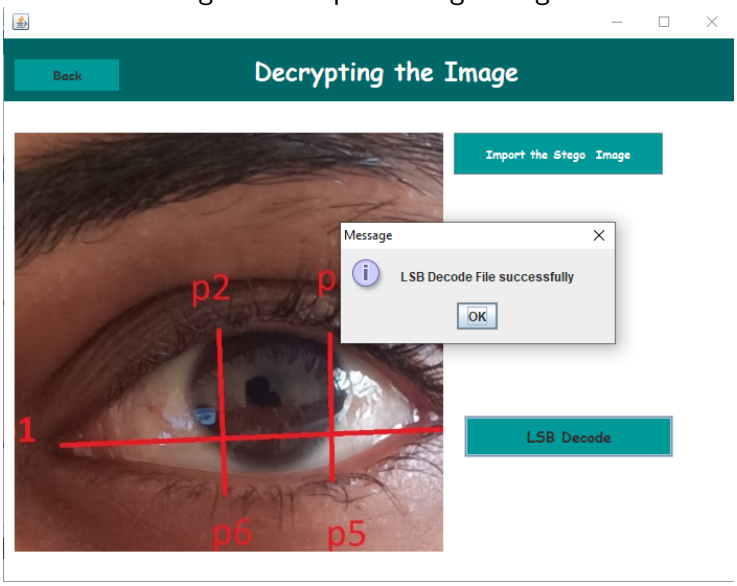


Figure 29: LZW Decompression

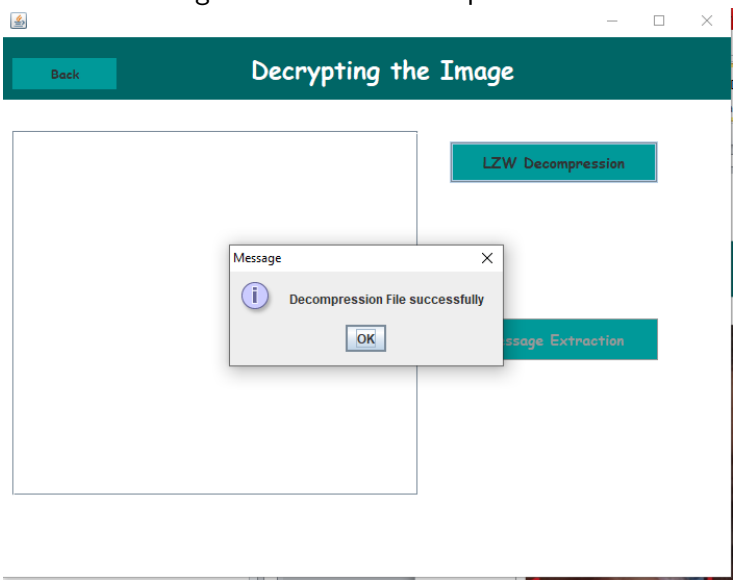
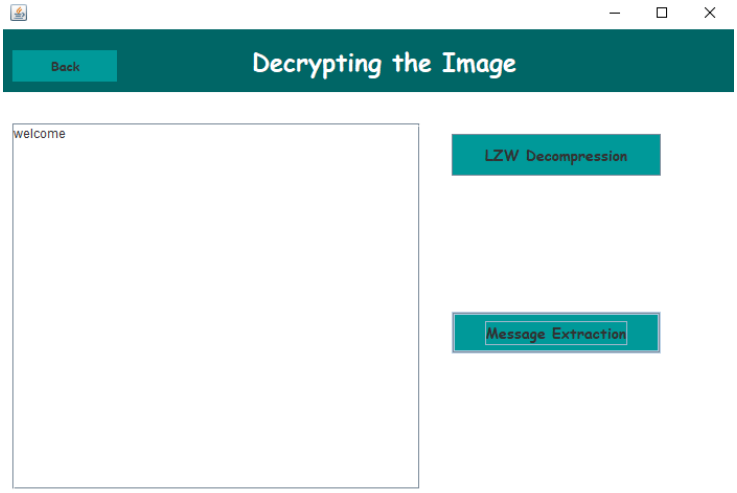


Figure 30: Decrytion of Data



CHAPTER 9: CONCLUSIONS

9.1 CONCLUSION

The main aim of the proposed system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. The proposed system will solve cloud storage issues of data security using cryptography and steganography techniques. And data security will be achieved using ECC and AES algorithm and key information will be safely stored using LSB technique (Steganography) as well as less time will be used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we will accomplish better data integrity, high security, low delay, authentication, and confidentiality. This project will successfully combine two of the security techniques: cryptography and steganography to provide double security for stored data in the cloud environment. We have presented hybrid encryption where symmetric algorithm AES combine with ECC is used to secure stored data in the cloud. The results of the encryption of secret data are then hidden in the image using the LSB algorithm after encrypted compression data. In this project proposal, the amount of data hidden in the image increases while the distortion on the image is reduced compared to the results of data concealment without compression using the LSB algorithm. This system will be more powerful and efficient for securing the data in the cloud environment. Besides, it will be more powerful to verify the integrity of data after retrieval from the cloud.

9.2 FUTURE WORK

Our proposed model contains a hybrid cryptography algorithm that efficiently encrypts the transmitted data through the cloud. Firstly, our hybrid cryptography algorithm will present a variety of different encrypting algorithms that allow the user to choose the encrypting method which is suitable with his own type of data. Secondly, the hybrid cryptography algorithm will improve the performance of the encryption algorithms since it encrypts the data in a minimum time and in a secure way. Thirdly, the proposed hybrid cryptography algorithm will allow the users to send and receive data in a secure way without facing the problem of attacking data. As a future work, new hybrid algorithms can be constructed from different existence algorithms to improve the encryption process and compare it with the results of our current work.

9.3 APPLICATIONS

- Reducing the complexity in generating a key.
- Reducing the key size by using the LZW compression technique.
- Hiding the key by implementing steganography through LSB algorithm.
- Using AES in combination with ECC can do a lot better with the optimization and security of the data.

- We can use this application for securing the files and audio from unauthorized user/hacker etc.
- This application can use in cybercrime for investigation and secure storage of video, files and Audio etc.
- This can be used in military to store and secure sensitive data.

APPENDIX A: FEASIBILITY ASSESSMENT

For evaluating the proposed system's performance, several RGB images will be used as cover images and hide a message containing a different number of characters in each cover image. Then, the evaluation is performed through the calculation of the signal-to-noise ratio (PSNR) as a parameter. Equation "(1)" is used to calculate the value of PSNR, but first, the value of Mean Square Error (MSE) is needed to be calculated according to Equation "(2)". The structural similarity index (SSIM) matrix of the stego-image is also calculated using Equation "(3)" where SSIM refers to the symmetry between the cover image and the misleading image of the information steganography technology.

$$\mathbf{PSNR} = \mathbf{10log_{10}}\frac{\mathbf{C max^2}}{\mathbf{MSE}}$$

Where,

max C indicates the maximum value holds in the image

$$\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{mn}}\sum_{\mathbf{i=1}}^{\mathbf{m}}\sum_{\mathbf{j=1}}^{\mathbf{n}}(\mathbf{C}-\mathbf{S})^{\mathbf{2}}$$

Where,

C is the cover image, and S is the stego-image. m, n are number of rows and columns of the cover image and the stego-image

$$\mathbf{SSIM}(\mathbf{x},\mathbf{y}) = \frac{(\mathbf{2_{xy}}+\mathbf{c_1})(\mathbf{2v_{xy}}+\mathbf{c_2})}{(\mathbf{^2_x}+\mathbf{^2_y}+\mathbf{c_1})(\mathbf{v_x^2}+\mathbf{v_y^2}+\mathbf{c_2})}$$

Where,

is average values of x,

y Vx and Vy are the standard deviation,

and Vxy is the cross-covariance for the image.

APPENDIX B:

Details of paper publication: name of the conference/journal, comments of reviewers, certificate, paper.

No paper published yet.

APPENDIX C: PLAGIARISM REPORT

Plagiarism Checker X - Report

Originality Assessment

11%

Overall Similarity

Date: May 23, 2023
Matches: 1628 / 14308 words
Sources: 50

Remarks: Low similarity detected, check with your supervisor if changes are required.

Verify Report:
Scan this QR Code

v 8.0.11 - WML 4
FILE - REPORT-1.PDF

A PROJECT REPORT ON ENCRYPTION OF CLOUD DATA USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF ENGINEERING (COMPUTER ENGINEERING) SUBMITTED BY STUDENT NAME EXAM NO. Ayush Bolla B190074209 Deep Pawar B190074255 Pranit Rathod B190074258 Vishaka Matkar B190074243 Under the guidance of Prof. D. D. Sapkal 25 DEPARTMENT OF COMPUTER ENGINEERING PVG's COLLEGE OF ENGINEERING AND TECHNOLOGY & G K PATE(WANI) INSTITUTE OF MANAGEMENT 44, VIDYANAGARI, PARVATI, PUNE 411009 SAVITRIBAI PHULE PUNE UNIVERSITY 2022-23 Department of Computer Engineering, PVG COET & GKPIM 2022-23 i

CERTIFICATE This is to certify that the project report entitles "ENCRYPTION 10 OF CLOUD DATA USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY" Submitted by STUDENT NAME EXAM NO. Ayush Bolla B190074209 Deep Pawar B190074255 Pranit Rathod B190074258 Vishaka Matkar B190074243 is a bonafide student of this institute and the work has been carried out by him/her under the supervision of Prof. D D Sapkal and it is approved for 26 the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of Bachelor of Engineering (Computer Engineering). Prof. D. D. Sapkal Prof. D. D. Sapkal Dr. M R Tarambale Guide Head of Department I/C Principal, Place: Pune Date: 3 Department of Computer Engineering, PVG COET & GKPIM 2022-23 ii

Acknowledgement It gives us great pleasure in presenting the Project Work - I report on "Encryption 10 of cloud data using hybrid cryptography and steganography" and to express my deep regards towards those who have offered their valuable time and guidance in our hour of need. 48 I would like to express my sincere and wholehearted thanks to our project guide and Head of the department Prof. D.D.Sapkal for contributing valuable time,

Sources

1	https://www.techtarget.com/searchsoftwarequality/definition/waterfall-model INTERNET 1%
2	https://sandilands.info/nsl/CryptographyAssumptionsandPrinciples.html INTERNET 1%
3	https://www.pvgcoet.ac.in/academics/departments/computer-engineering/ INTERNET 1%
4	https://www.mdpi.com/2079-9292/10/21/2673/htm#:~:text=The proposed hybrid model (AES-ECC) is used to,the security of the system in less time. INTERNET 1%
5	https://www.1000sourcecodes.com/2012/05/software-engineering-risk.html INTERNET 1%
6	https://www.geeksforgeeks.org/introduction-to-java-swing/ INTERNET 1%
7	https://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm INTERNET 1%
8	https://www.javatpoint.com/software-engineering-data-flow-diagrams INTERNET <1%
9	https://thesai.org/Downloads/Volume8No11/Paper_58-NHCA_Developing_New_Hybrid_Cryptography_Algorithm.pdf INTERNET <1%
10	https://ieeexplore.ieee.org/abstract/document/9142072 INTERNET <1%
11	https://www.researchgate.net/profile/A-Ospanova-3/publication/360034729_Social_Distance_Detection_and_Alert_System_using_Deep_Learning_and_Computer_Vision/links/625ea25da279ec5dd702b2af/Social-Distance-Detection-and-Alert-System-using-Deep-Learning-and-Computer-Vision.pdf INTERNET <1%
12	https://tallyfy.com/uml-diagram/ INTERNET <1%
13	https://www.analyticsvidhya.com/blog/2022/10/cloud-cryptography-a-reliable-solution-to-secure-your-cloud/#:~:text=By encrypting data stored in the cloud, cloud,between security and efficiency in their cloud computing. INTERNET <1%

14	https://testbook.com/question-answer/which-of-the-following-type-of-ciphers-is-shown-in--61a9fc4945c55a5ab1451b11 INTERNET <1%
15	https://www.rroij.com/open-access/next-generation-method-for-reversible-datahiding.php?aid=50983 INTERNET <1%
16	https://www.geeksforgeeks.org/dbms/ INTERNET <1%
17	https://www.techtarget.com/searchdatamanagement/definition/hashing INTERNET <1%
18	https://www.geeksforgeeks.org/cryptography-in-blockchain/ INTERNET <1%
19	https://www.techtarget.com/whatis/definition/LZW-compression#:~:text=LZW compression is a method to reduce the,also suitable for compressing text and PDF files. INTERNET <1%
20	https://www.ibm.com/docs/ssw_ibm_i_72/rzahg/rzahg3aau1.htm INTERNET <1%
21	https://www.scribd.com/document/637105041/The-Design-and-Implementation-of-a-Secure-File-Storage-on-the-Cloud-using-Hybrid-Cryptography INTERNET <1%
22	https://www.researchgate.net/publication/338599091_A_Hybrid_Encryption_Algorithm_for_Security_Enhancement_of_Wireless_Sensor_Networks_A_Supervisory_Approach_to_Pipelines INTERNET <1%
23	https://geekflare.com/challenges-and-risks-in-cloud-computing/ INTERNET <1%
24	https://www.ijraset.com/research-paper/secure-the-file-storage-on-cloud-computing INTERNET <1%
25	https://www.pvgcoet.ac.in/ INTERNET <1%
26	https://www.coursehero.com/file/128439465/Tic-Tac-Toe-Documentationdocx/ INTERNET <1%
27	https://www.geeksforgeeks.org/unified-modeling-language-uml-introduction/ INTERNET <1%

28	https://scholar.google.com/citations?user=Ob2liOAAAAAJ INTERNET <1%
29	https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-credential?view=powershell-7.3 INTERNET <1%
30	https://en.wikipedia.org/wiki/Non-functional_requirement INTERNET <1%
31	https://article.sciencepublishinggroup.com/pdf/10.11648.j.ajcst.20220502.13.pdf INTERNET <1%
32	https://iq.opengenus.org/lempel-ziv-welch-compression-and-decompression/ INTERNET <1%
33	https://www.ijert.org/research/implementation-of-lsb-steganography-and-its-evaluation-for-various-file-formats-lsb-jsteg-IJERTV2IS60823.pdf#:~:text=The Least Significant Bit (LSB) embedding technique suggests,images in 24-Bit, 8- Bit, Gray scale format. INTERNET <1%
34	https://ieeexplore.ieee.org/abstract/document/8852633 INTERNET <1%
35	https://dl.acm.org/doi/abs/10.1109/TrustCom.2012.87 INTERNET <1%
36	https://aws.amazon.com/what-is/mfa/ INTERNET <1%
37	https://myonlinevidhya.com/cryptography/ INTERNET <1%
38	https://www.ibm.com/docs/en/arl/9.7?topic=shapes-sequence-diagrams INTERNET <1%
39	https://www.geeksforgeeks.org/introduction-to-java/ INTERNET <1%
40	https://ijariie.com/AdminUploadPdf/Achieving_Cloud_Security_Using_Hybrid_Cryptography_Algorithm_ijariie6850.pdf INTERNET <1%
41	https://security.stackexchange.com/questions/171302/can-data-be-decrypted-with-the-public-key-if-encrypted-with-the-private-key INTERNET <1%

REFERENCES

1. C.A.Subasini, Dr. S. Nikkath Bushra, "Securing of Cloud Data with Duplex Data Encryption Algorithm," Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC 2021) IEEE Xplore, Part Number: CFP21K25-ART
2. Raj Parab, Anwit Paul, UrjitMojumdar, Rahul Patil, "Secured Cloud Storage Using Hybrid Cryptography," International Research Journal of Modernization in Engineering Technology and Science, e-ISSN: 2582-5208
3. Mustafa S. Abbas, Suadad S. Mahdi, Shahad A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography,"2020 International Conference on Computer Science and Software Engineering (CSASE) IEEE Xplore
4. Uttam Kumar, Mr. Jay Prakash, "Secure File Storage on Cloud Using Hybrid Cryptography Algorithm," International Journal of Creative Research Thoughts (IJCRT) IJCRT2007048, ISSN: 2320-2882
5. Chi Chen at. Al. proposed An Efficient Privacy-Preserving Ranked Keyword Search Method IEEE 2016.
6. Li, Jiayi, et al. "Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data." IEEE Transactions on Cloud Computing (2020).
7. Dai, Xuelong, et al. "An efficient and dynamic semantic-aware multikeyword ranked search scheme over encrypted cloud data." IEEE Access 7 (2019): 142855-142865.
8. Lichun Li at. al. Privacy-Preserving-Outsourced Association Rule Mining on Vertically Partitioned Databases in AUGUST 2016.
9. Chunhua Su at. al. proposed Analysis and Improvement of Privacy-Preserving Frequent Item Protocol for Accountable Computation Framework IEEE 2012.

REPORT DOCUMENTATION

Report Code: CS-BE-Project 2022-2023		Report Number: 14	
Report Title: Encryption of cloud data using Hybrid Cryptography And Steganography			
Address (Details): PVG's College of Engineering & Technology and GKPIM, Pune Pin – 411009, State: Maharashtra, INDIA.			
Author 1 : Ayush Bolla **Address:** 21, Kap-Kaneri, Near BNMC Office, Old ST Stand, Bhiwandi,Thane - 421302 **Phone:** 7798760091 **E-mail:** ayushbolla07@gmail.com **Roll No:** B190074209	**Author 2 :** Deep Pawar **Address:** SrNo.31/5, Chandradeep, Laygude Wasti, Dhayari, Pune-41 **Phone:** 9284429917 **E-mail:** deepcpawar28@gmail.com **Roll No:** B190074255	**Author 3 :** Pranit Rathod **Address:** Tirupati scheme enclave, Jalan Nagar, Near public garden, railway station, Aurangabad-431005 **Phone:** 8149462064 **E-mail:** pranitrathod007@gmail.com **Roll No:** B190074258	**Author 2 :** Vishakha Matkar **Address:** B1 Prince Farm House,Aatiyawad Dabhel Daman -396215 **Phone:** 8128074687 **E-mail:** matkar.vishakha@gmail.com **Roll No:** B190074243
Year:2022-2023 **Branch:** Computer Engineering			
Keywords: Cloud Computing, Steganography, Cryptography, AES, ECC, LZW, LSB, SHA			
Type of Report: FINAL	**Report Checked By:**	**Report Checked Date:**	**Guides Complete Name:** Prof. D. D. Sapkal	**Total Copies:** 5