Image and Text Encrypted Data with Authorized Deduplication in Cloud

A.R. Uphade[1], V.P. Niwane[2], R.M. Yadav[3], S.A. Mandavkar[4], S.R. Patil [5], S.A. Badarkhe[6]

Department of Electronics and Telecommunication Engineering, SKNCOE, SPPU, Pune, Maharashtra

[1]akshayuphade3642@gmail.com
[2]vivek.niwane_skncoe@sinhgad.edu
[3]yadavrushikesh.ry@gmail.com
[4]shubham.mandavkar02@gmail.com
[5]gk.sujata@gmail.com
[6]smita.garde_skncoe@sinhgad.edu

Abstract— **An abstract is a brief summary or condensed version of the entire project, in this Project we Use Machine Learning Technique and Algorithm for the Implementation. We USE AES and MD5 Algorithm For the encryption and Decryption. after Image and Text Encryption Done Then Generate ciphers. And enter Key Sent To mail. Cloud computing is network-based computing system and it is the large storage space area where the authorized user can access the platform from anywhere and anytime with the good internet or network connectivity. Cloud computing is mainly to shared resources, hardware, software applications to provide the device with on demand. It is like a remote server on the internet to store, manage, and process data instead of using desktop. So, the working period is faster when compared to other local computers. Cloud computing is the information technology services and product. It supports the virtualized resources, which is based on the reusability of IT infrastructure. Cloud Computing is the sequence of all required hardware, software, platform, applications, infrastructure and storage only with online identification.**

Keywords— **Machine Learning, AES, MD5**

I. INTRODUCTION

The role re-encryption is used to avoid the privacy data leakage and also to avoid the deduplication in a secure role re-encryption system (SRRS). And also, it checks for the proof of ownership for to identify whether the user is authorized user or not. This is for the efficiency. Role re-encryption method is to share the access key for the corresponding authorized user for accessing the particular file without the leakage of privacy data. In our project we are using both the avoidance of text and digital images. For example, we have the personal images in our mobile, handheld devices, and in the desktop etc., So, as these images have to keep secure and so we are using the encryption for to increase the high security. The text file also important for the users now-a-days. It has to keep secure in a cloud server. Digital images have to be protected over the communication, however generally personal identification details like copies of pan card, Passport, ATM, etc., to store on one's own pc. So, we are protecting the text file and image data for avoiding the duplication in our proposed system

II.RELATED WORK

A. *LITERATURE REVIEW*

Dawei Wang, Pinyi Ren and Qian Xu, Qinghe Du in order to secure the primary privacy information and provide quality- of-service provisioning for the secondary system, we propose a secondary encryption secure transmission scheme. In the proposed scheme, the primary system utilizes the secure secondary messages to encrypt the primary confidential messages and the secondary system can acquire some spectrum opportunities. Specifically, when the primary system is secure, the primary

information can be directly transmitted; when the primary system is insecure while the secondary messages can be securely trans-mitted, the primary system utilizes the secure secondary messages to encrypt the primary information; otherwise, the spectrum will be utilized for secondary trans- mission. For the proposed scheme, we investigate the performances of the primary ergodic secrecy rate and the average secondary throughput. Numerical results have demonstrated that the secondary encryption secure transmission scheme can secure the primary privacy messages and improve the secondary transmission throughput. [1]

Wen-Chung Kuo, Wan-Hsuan Kao, Chun-Cheng Wang, Yu-Chih Huang in the world of information development, the transmission of information is much more convenient. However, the transmission process always faces the risk of being attacked, stolen and tampered, which leads to the doubt that the data source is incorrect. For this reason, some scholars proposed to protect important information in the form of passwords. Alok et al. Proposed 3D-Playfair Cipher with

Message Integrity using MD5. This paper uses 3D-Playfair encryption for en- crypton. However, simple 3D-playfair encryption cannot guarantee the integrity of data during transmission, so the author proposes Combined with MD5 to ensure the integrity of the data, but there are doubts about the credibility of the data source, so this paper uses XOR calculation methods to further verify the credibility of the data. When a man-in-the- middle attack is encountered, the attacker intercepts the packet and tampering with the data content can still accurately determine whether the source of the data is the original sender. This method guarantees the integrity of the data while improving the credibility of the data.[2]

K. Jagruth, V. M. Manikandan reversible data hiding is widely studied in recent years due to its wide applications in various domains such as medical image transmission and cloud com- puting. In this manuscript, we propose a novel scheme for performing reversible data hiding in encrypted images. In this scheme, the data hider can embed one-bit additional data bit in a small block (B × 2 pixels) from the encrypted image. All the non-overlapping regions (blocks) in the encrypted image will be processed by accessing those blocks in a predefined order. To embed a bit value 0 in an encrypted image block, no need to modify any pixel values. If we want to embed bit value 1, all the pixels in the first column of the selected image block will be mapped into a new pixel value based on a predefined function. At the receiver side, the data extraction and image recovery are carried by comparing the closeness between pixels in the adjacent columns of the pixels in each block of the decrypted image.[3]

H. Kevin Ronaldo Cahyono, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto This research proposes a combination of dual protection on text messages transmission using Chinese Remainder Theorem (CRT) steganography and Rivest Cipher 4 (RC4) encrypting method. This combination aims to optimize the performance of encryption and message insertion into an image. Security This message is done by encrypting text messages using RC4 first, then the results are embedded in the grayscale type container image with the CRT method. The evaluation standards that will be used in this research are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), and Character Error Rate (CER). MSE, PSNR and SSIM are used as a measure of the quality of stage images. To determine the performance of the proposed method, message insertion is carried out in three types of sizes, namely maximum payload, half payload and one quarter payload. While the CER is used to find out the results of decryption of text messages. The resulting CER value is 0, this indicates the message was extracted and decrypted perfectly. [4]

Madhu D, S Vasuhi steganography is a study of invisible communication that typically addresses how the message is concealed. Protection is required when we want to send data across any medium, this is why steganography has been built to safely send data in an image where the human eyes cannot identify it. This paper integrates cryptography and steganography through an image processing technique. YCbCr color model based on the 2-bit XOR LSB image steganography is proposed here in. The proposed scheme is a very safe technique for data concealed in the spatial field for image steganography, which converts an image from the color of RGB to the YCbCr space, and then secret data is concealed inside in the Cr color space component using 2-bit XOR.[5]
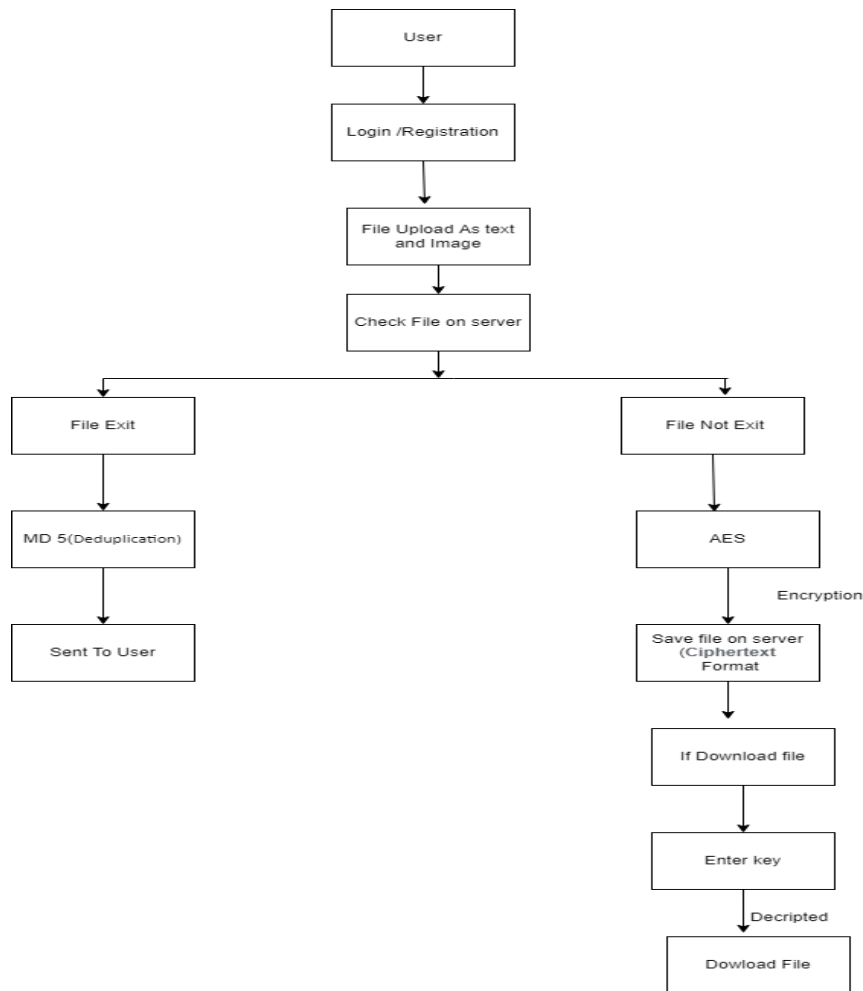
III.SYSTEM ARCHITECTURE

Fig 1: System architecture

1. Module

- Admin

- In this module, the admin has to log in by using valid user name and password. After login successful he can do some operations, such as View All Users and Authorize, View All E-Commerce Website and Authorize, View All Products and Reviews, View All Products Early Reviews, View All Keyword Search Details, View All Products Search Ratio, View All Keyword Search Results, View All Product Review Rank Results.

- View and Authorize Users

- In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, username, email, address and 17 admin authorize the users.

- View Charts Results

- View All Products Search Ratio, View All Keyword Search Results, View All Product Review Rank Results.

- Ecommerce User

- In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password Once Login is successful user will do some operations like Add Products, View All Products with reviews, View All Early Product's reviews, View All Purchased Transactions.

- End User

- In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will best or to the database. After registration successful, he has to login by using authorized user

name and password. Once Login is successful user will do some operations like Manage Account, Search Products by keyword and Purchase, View Your Search Transactions, View.

2. Data Flow Diagram

In Data Flow Diagram, we Show that flow of data in our system in DFD0 we show that base DFD in which rectangle present input as well as output and circle show our system, In DFD1 we show actual input and actual output of system input of our system is text or image and output is rumor detected like wise in DFD 2 we present operation of user as well as admin.

Fig 2: Data Flow Diagram
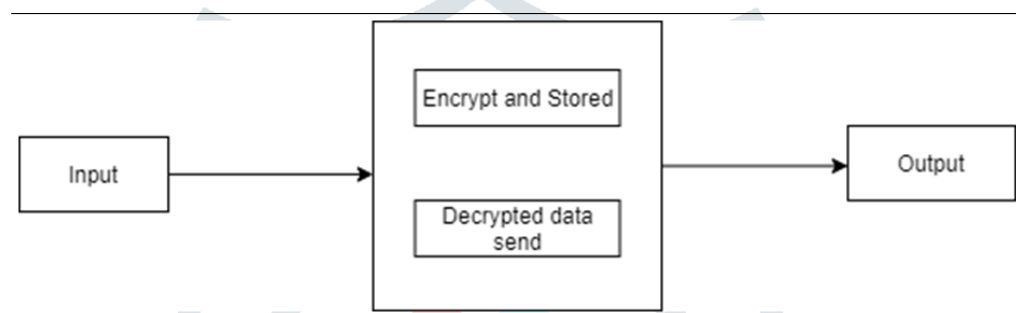
Fig 3: Data Flow Diagram
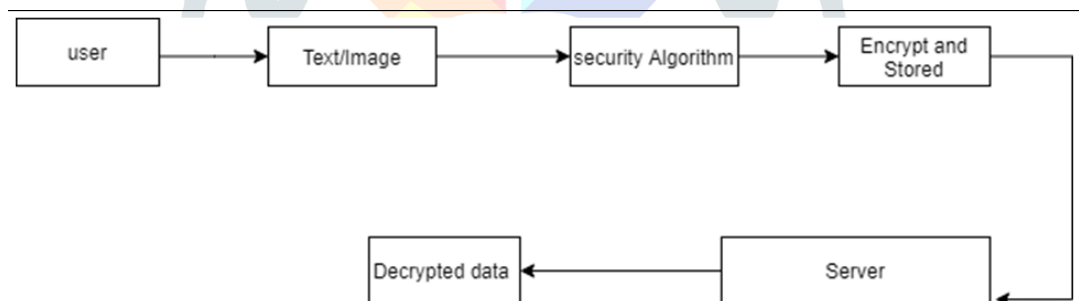
Fig 4: Data Flow Diagram

3. UML DIAGRAMS

Unified Modelling Language is a standard language for writing software blueprints. The UML may be used to visualize, specify, construct and document the artifacts of a soft- ware intensive system. UML is process independent, although optimally it should be used in process that is use case driven, architecture-centric, iterative and incremental. The Number of UML Diagram is available.

4. Class Diagram.

Class diagrams are the blueprints of your system or subsystem. You can use class diagrams to model the objects that make up the system, to display the relationships between the objects, and to describe what those objects do and the services that they provide. Class diagrams are useful in many stages of system design.
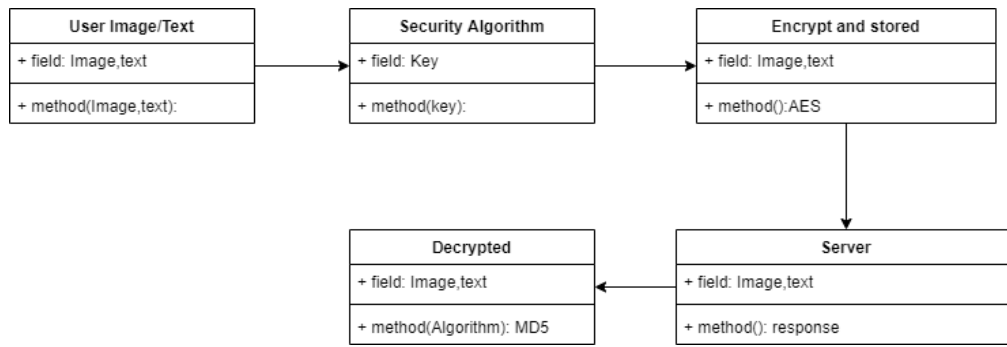
Fig 5: Class Diagram.

5. Use case Diagram

In the design of a system, a number of classes are identified and grouped together ina class diagram that helps to determine the static relations between them. In detailed modelling, the classes of the conceptual design are often split into subclasses.
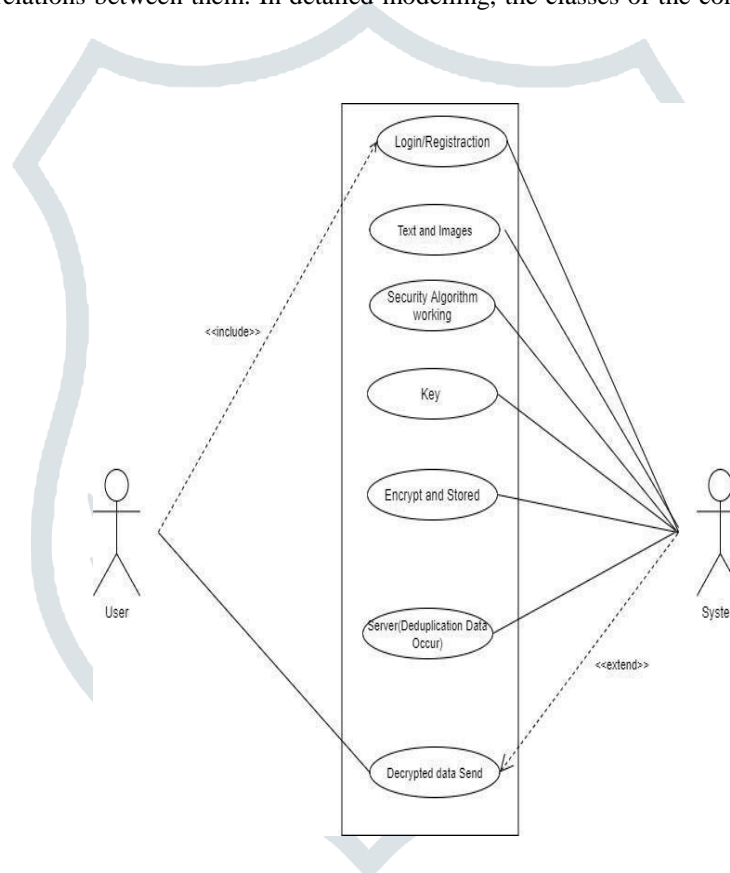

Fig 6: Use case Diagram

6. Activity Diagram.

An activity diagram shows business and software processes as a progression of actions. These actions can be carried out by people, software components or computers. Activity diagrams are used to describe business processes and use cases as wellas to document the implementation of system processes.
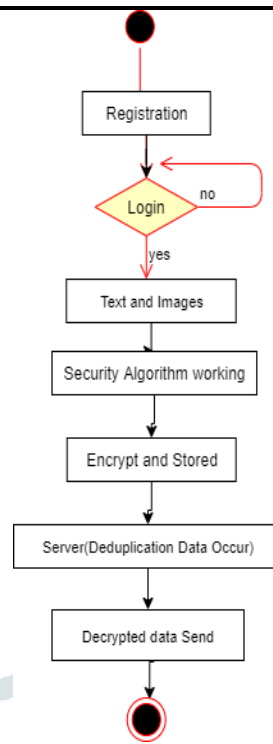
Fig 7: Activity Diagram

7. Sequence Diagram.

A sequence diagram is a type of interaction diagram because it describes how—and in what order—a group of objects works together. These diagrams are used by soft-ware developers and business professionals to understand requirements for a new system or to document an existing process.
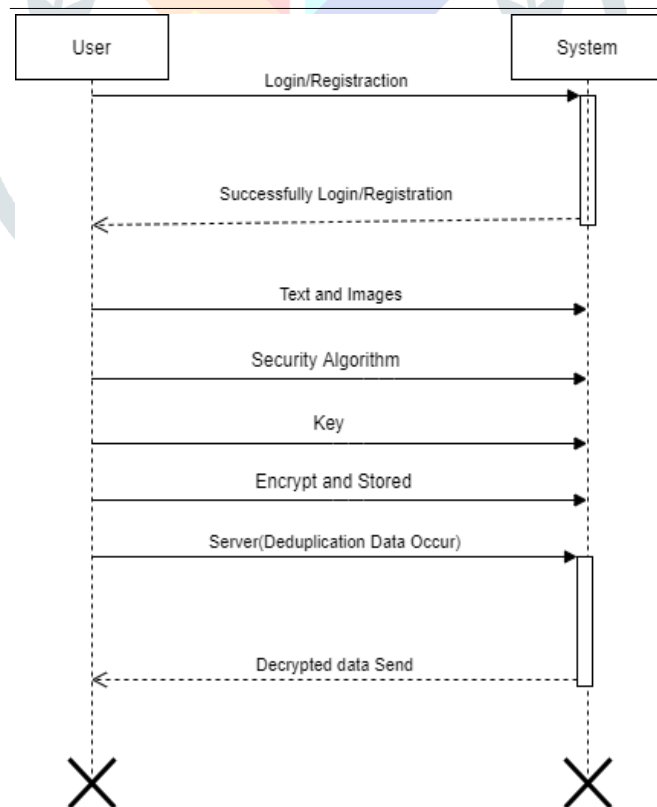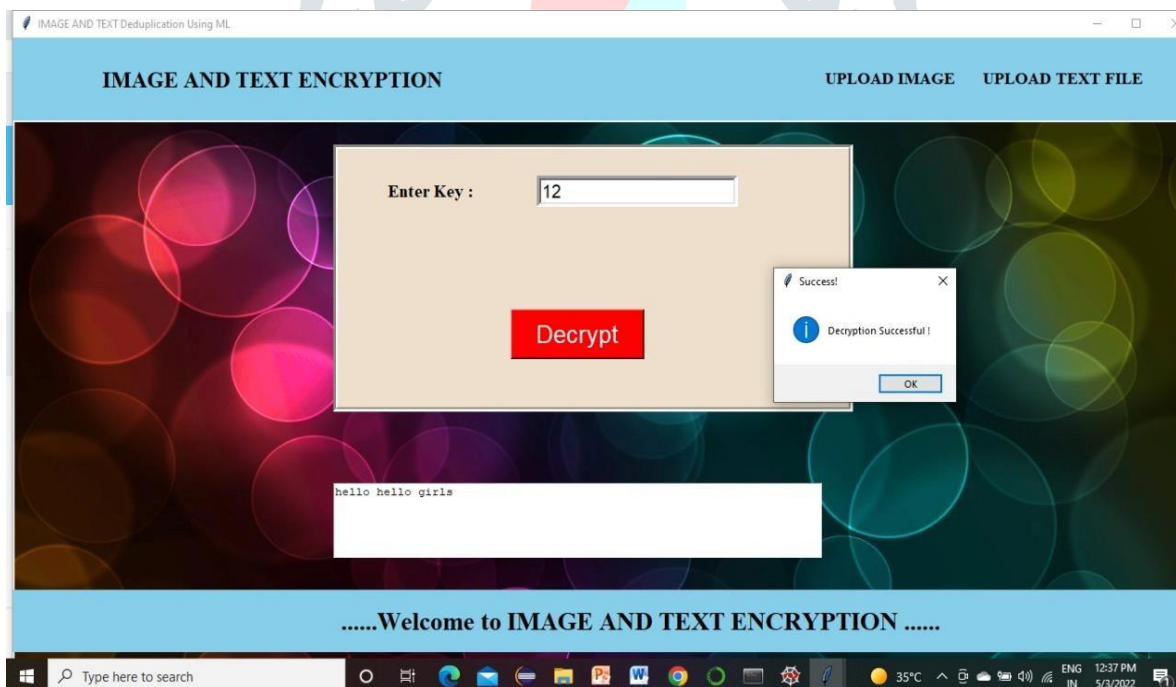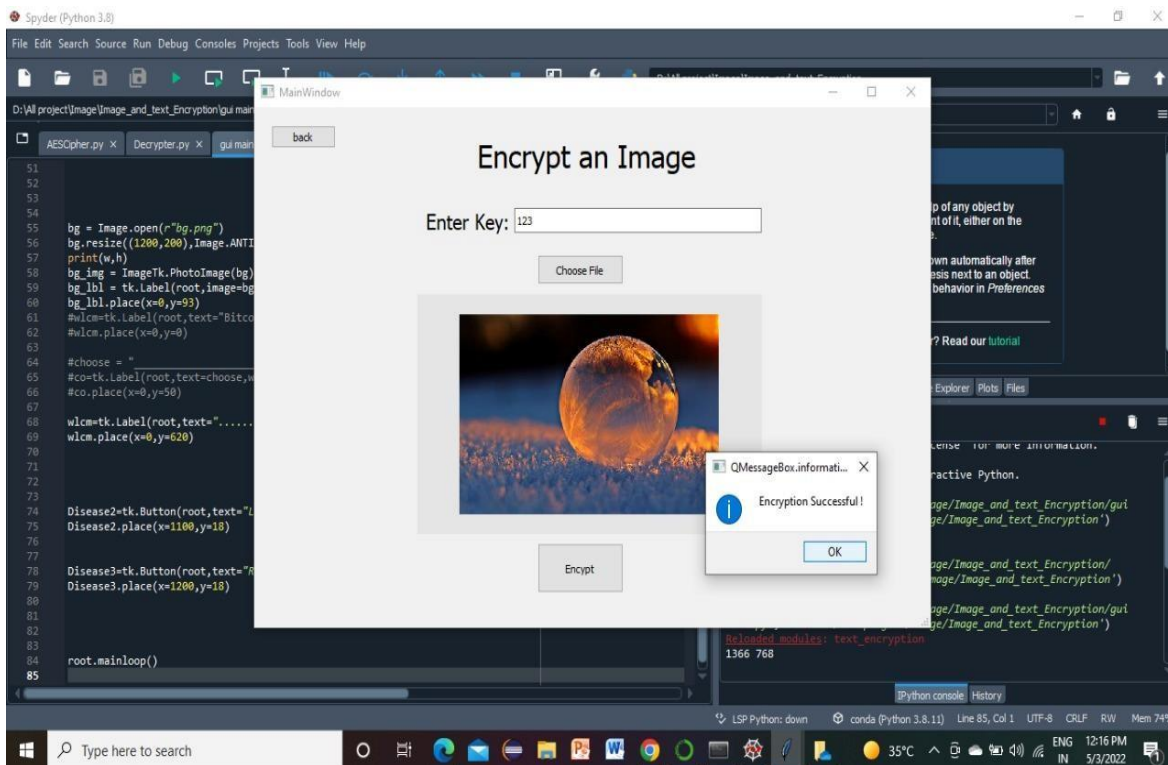
Fig 8: Sequence Diagram

IV. RESULT

V. CONCLUSION

We discussed that to avoid the duplication using the Encryption And de-crypton method. And for the text uploading we are using three algorithms, For the uploading in the cloud system we are using the Structural Similarity ml Algorithm and the main purpose of the similarity index is to check the image quality such as luminance, contrast and structure, then it measures the similarity of two image. To store large amount of data with efficiency, to avoid the duplicate text and image we are using the encryption method.

ACKNOWLEDGEMENT

REFERENCES

[1]   Subhash Chand Agrawal; Rajesh Kumar Tripathi; Anand Singh Jalal Human-fall detection from an indoor video surveillance Published in: 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) Date of Conference: 3-5 July 2017 Date Added to IEEE Xplore: 14 December 2017

[2]   Zhanyuan Huang; Yang Liu ; Yajun Fang ; Berthold K. P. Horn Videobased Fall Detection for Seniors with Human Pose Estimation Published in: 2018 4th International Conference on Universal Village (UV) Date of Conference: 21-24 Oct. 2018 Date Added to IEEE Xplore: 14 February 2019

[3]   Yie-Tarng Chen; Yu-Ching Lin; Wen-Hsien Fang A hybrid human fall detection scheme Published in: 2010 IEEE International Conference on Image Processing Date of Conference: 26-29 Sept. 2010 Date Added to IEEE Xplore: 03 December 2010

[4]   Priyanka S. Sase; Smriti H. Bhandari Human Fall Detection using Depth Videos Published in: 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN) Date of Conference: 22-23 Feb. 2018 Date Added to IEEE Xplore: 27 September 2018

[5]   Shugang Zhang; Zhen Li; Zhiqiang Wei ; Shuang Wang An automatic human fall detection approach using RGBD cameras Published in: 2016 5th International Conference on Computer Science and Network Technology (ICCSNT) Date of Conference: 10-11 Dec. 2016 Date Added to IEEE Xplore: 19 October 2017