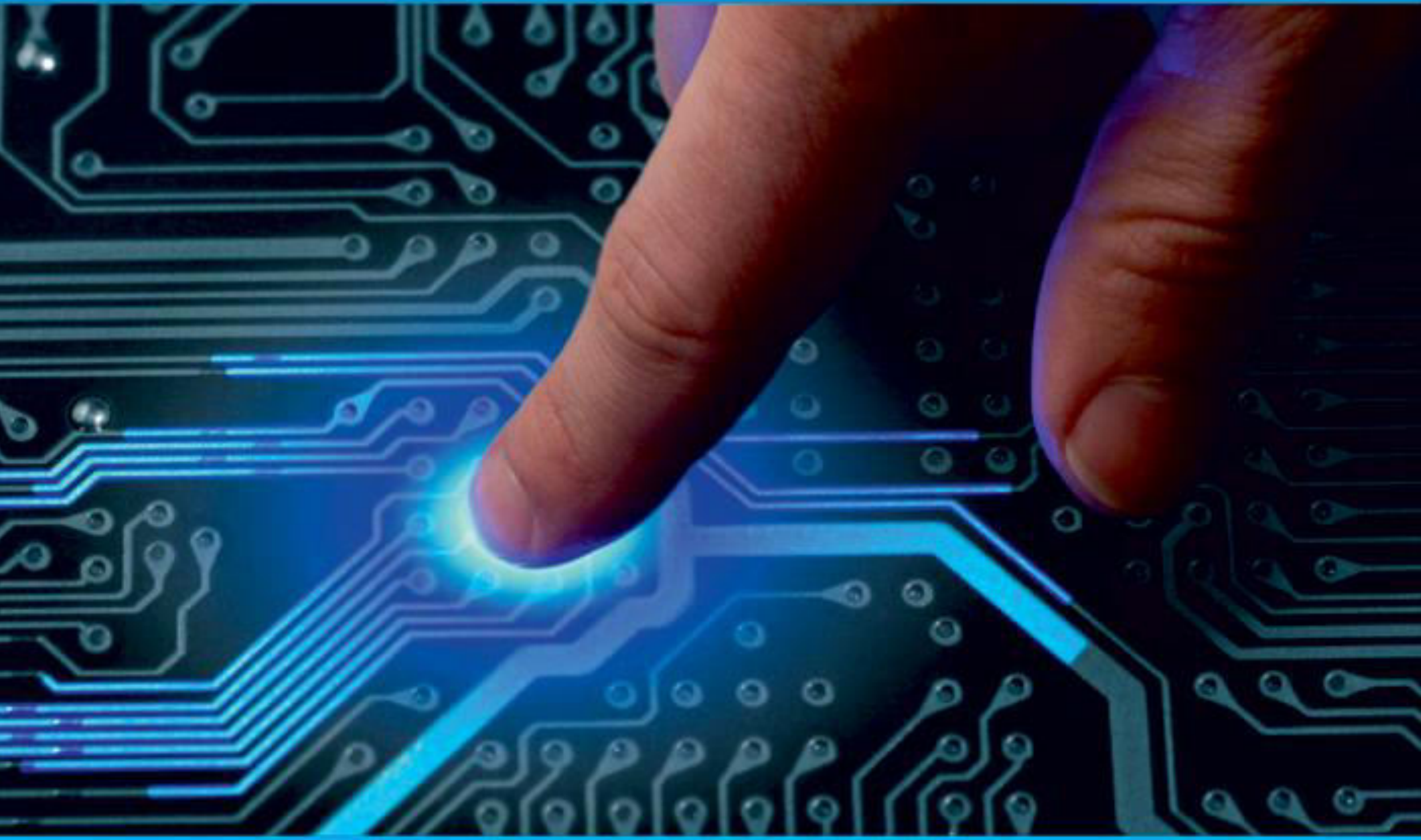
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

Encryption of Data with Authorized Deduplication in Cloud

Sonu Gaikwad[1], Aishwarya Bijja[2], Nishant Gawali[3], Somnath Bhosale[4],

Prof. Prachi Waghmare[5]

Department of Computer Science and Engineering, Nutan College of Engineeringand Research, Pune, Maharashtra, India[1-4]

Assist. Professor & IIIC Co-ordinator, Department of Computer Science and Engineering, Nutan College of Engineeringand Research, Pune, Maharashtra, India[5]

ABSTRACT: Storing the data is the most essential service of cloud. Data that we store on the cloud in the form of text or images need to be secured. Here comes the role of Re-encryption and deduplication which are the most important factors to store data in the cloud without data leakage and deduplication. It will find the proof of the owner to recognize whether the user is authorized or not. This is efficiency. Re-Encryption: The data that is stored in the cloud should be secured without the access ofunauthorized users. Then comes the data security or re-encryption method to maintain the user's data privacyand data securely stored in the cloud. The re-encryption role is to share the access key only with an authorized user for accessing the file without the data leakage problem. Deduplication: We are protecting the text files and images by removing the deduplication in our purposed system. The resultscan be predicted the possible efficiency and effectiveness of the scheme for the possible practical deployment of data deduplication in cloud storage. For example, we have tons of personal individual images, and text files on our cell phones, PCs, Laptops, etc., So, these images and text files need to be secure for that we are using encryption to increase security. Aside from reducing overburden the cloud system has many spots for data privacy and cloud users' privacy. However generally personal identifications like pan cards, Aadhar cards, passports, ATM copies, etc., need to keep secure on the cloud server. For avoiding deduplication and protecting our data we are proposing this.

KEYWORDS*: Deduplication, encryption and decryption, Cloud computing, Cipher text*

I. INTRODUCTION

Cloud Computing is the computing system and storage area over the network where only authorized users can access the platform from anywhere and everywhere using internet connectivity. As we know datastorage is the most valuable thing in a cloud system. Cloud is the server on the internet for storing, managing and processing the data instead of using a desktop/computer, Laptop, and so on.

The proposal of this project is related to cloud computing, these clouds have a large amount of data storage that is accessible at low costs as well as data and files that are stored on clouds that are independent of the platform for accessing the files. All of these functions of the cloud have been attractive to users use cloudservices in the last few years of leading to a large amount of data being stored. This has to be a huge challenge for cloud service providers as well as to handle all this efficiently, the data deduplication technique came into the existence. This technique used is to minimize the data redundancy that is to get rid from duplicatecopies of the similar data which is stored in the cloud and through which most of the space gets utilized.

Data Encryption is used to determine malicious parties from accessing sensitive data. An important thing is to define Data encryption is the today's worlds of cybersecurity. To ensure that our data is safe on cloud, educate the organization on best practices that data usage and sharing of that data too.

To conquer this, a combination of encryption is the combination of keys for encryption/ decryption of the data and the key is by using cryptographical hash functions of the data. Subsequently generation of key to users will use the keys and send the that cipher text to the cloud. Through which, data copies produce the similar combination of keys. Also, for removing the access to data, the validation of authorization is much important to provide the proof that the user indeed owns the same file when a duplicate file found.

Hence this encryption technique enable us the data deduplication cloud and give us needed security for only authorized users.

Overview:

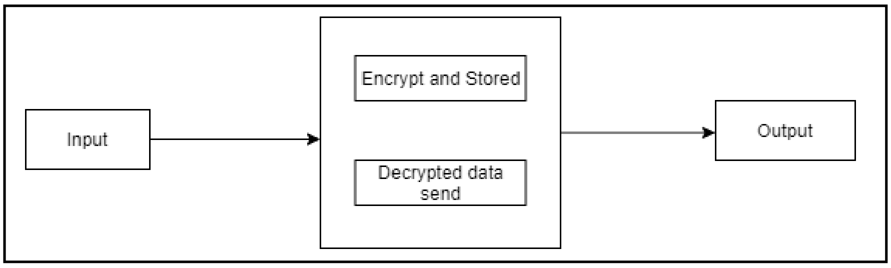


Fig 1:- Overview of encryption/decryption of data

II. NEED OF STUDY

The idea of this project is associate with cloud computing, a virtual storage space for the data which is used across the whole internet. These clouds have a huge data storage available in low costs and the data or files stored on the clouds are platform independent for accessing the files. All these functions of cloud have been attracting users more and more cloud services since past few years leading to large amount of data to be stored. This has to be as a big challenge for cloud service providers and to handle this efficiently, data deduplication technique has come into existence. This technique is used to minimize data redundancy that is to eliminate duplicate copies of same data stored on the cloud and through which more and more space utilization.

Personal photos, for instance, can be found on desktop computers, mobile and handheld devices, and so on. Therefore, in order to strengthen security for these photographs, we are implementing encryption.

Sr. No	Paper Name, Year	Author Name	Methodology/ Algorithms/	Datasets	Accuracy/ Results	Advantage	Future scope
1	Deduplication of Encrypted Big data in cloud 2016	Wenxiu Ding, Robert.H.Reng	Grant Access to Duplicate data	Text Data	Manages encrypted big data in cloud with deduplication based on ownership challenge and PRE	Flexibility Low cost of storage Big Data Support	Optimizing the design and implementation for practical deployment and studying verifiable computation to ensure that CSP behaves as expected in deduplication management
2	A deduplication Aware Resemblance Detection and Elimination	Wen Xia, Hong Jiang, Lie Tian	DARE Algorithm	Synthetic backup dataset Emacs-21.4	DARE can be a powerful & efficient tool for	data reduction In backup	Study and improve the data restore performance of storage systems

	Scheme for data Reduction with Low overheads 2015			GDB-6.7	maximizing data-reduction by further detecting resembling data with low overhead		based on deduplication and delta compression in future work
3	Boaff : Distributed Deduplication for Big Data storage in Cloud 2015	Shengmei Luo, Guangyan Zhang	Local Similarity routing Algorithm, Boafft's Data routing Algorithm	Web Dataset Mail Dataset VM Dataset	Improved data deduplication ratio Maintains similarity index table in memory	Scalable throughput and capacity	We will incorporate cache into other deduplication scheme, we will build a power measurement module.
4	Achieving Efficientprivacy preserving cross Domain Big Data de-duplication in cloud environment 2017	Kim Kwang, Raymond Choo, Fan Yin	Deduplication Decision Tree, Data deduplication over DDT-A	Text Data	Privacy-Preserving big data deduplication in cloud storage for three-tier cross domain architecture	Security can be achieved. Easy to find duplicate data in textual files	Includes extending the proposed scheme to fully protect the duplicate information from disclosure even by malicious CSP
5	Image and Text Encrypted with Authorized Deduplication in cloud 2020	S.Uthayashanagr, J.Abinaya, V.Harshini	Levenshetin distance algorithm, fuzzy match algorithm	Image and Text	To avoid the duplication using radix tree method	Store large amount of data with efficiency	____

III. RESEARCH METHODOLOGY

AES (Advanced Encryption Standard)

AES is a widely used symmetric encryption algorithm that operates on fixed-size blocks of data, commonly 128 bits. The methodology for encryption and decryption using AES includes the following steps: Figure 3.0 shows the overall structure of the AES encryption process. The cipher takes a plaintext block size of 128 bits or 16 bytes. Depending on the key length, the algorithm is referred to as AES-128, AES-192, or AES-256.

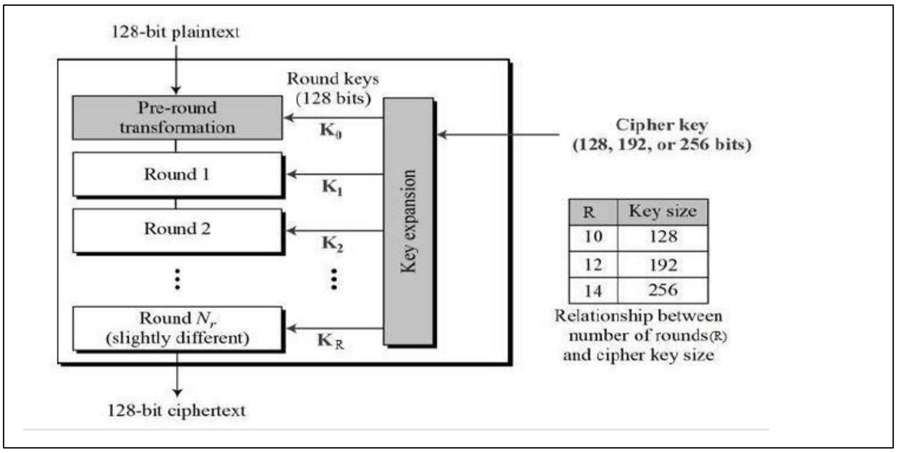


Fig 3.0 AES

MD5 Algorithm

The MD5 (Message Digest Algorithm 5) is a widely used cryptographic hash function. It takes an input message of arbitrary length and produces a fixed-size 128-bit hash value. MD5 is designed to be a one-way function, meaning it should be computationally infeasible to reverse the process and obtain the original message from its hash value.

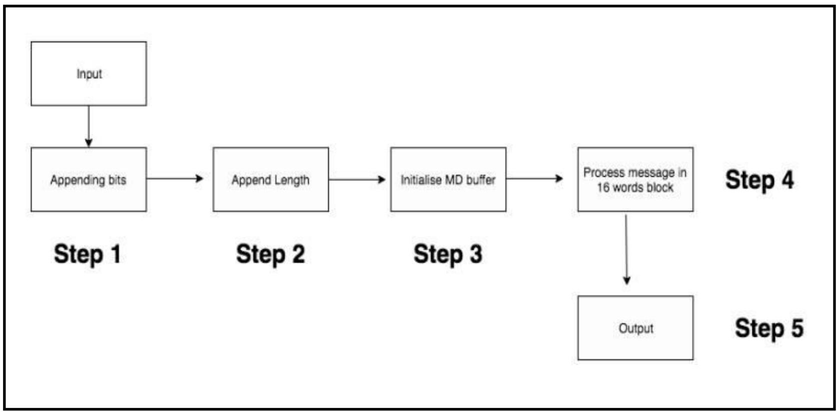


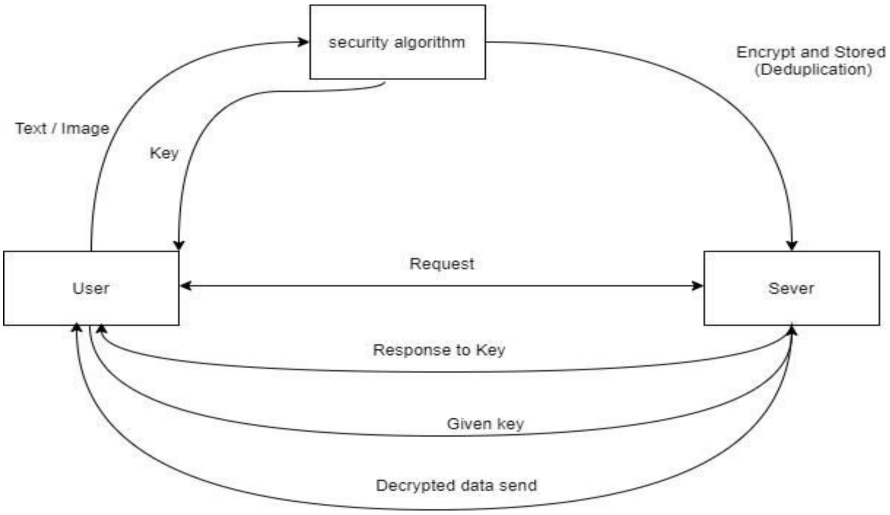
Fig 3.0.1

1.1 Proposed System

There are many reasons why encryption of data with authorized deduplication in cloud. Secure data deduplication uses AES and MD5 algorithms To determine if the user is an authorized user or not, it also looks for proof of ownership. This promotes effectiveness. The role re-encryption approach involves sharing the access key so that the appropriate authorized user can access the specific file without any privacy information leaking out. We are using both the avoidance of text and digital visuals in our effort.

- Deduplication: For the Deduplication we use MD5 Algorithm. If deduplication Occur in file, then we sent to user again and if file contain is not deduplication, then store file.
- Encryption: File contain is unique That time AES algorithm working and store file in encrypted format.
- Decryption: If user want or access file or download file in original format that time AES algorithm download file in decrypted format

System Architecture :



2. Implementation

We are glad to inform that the Cloud Computing model Encryption of data with Authorized deduplication in cloud has been successfully build, utilizing AES and MD5 Algorithms and with the reference of architecture design and new technologies that have been demonstrated significant performance benefits over previous techniques. The system has been tested well and we are delighted to show off the application interface

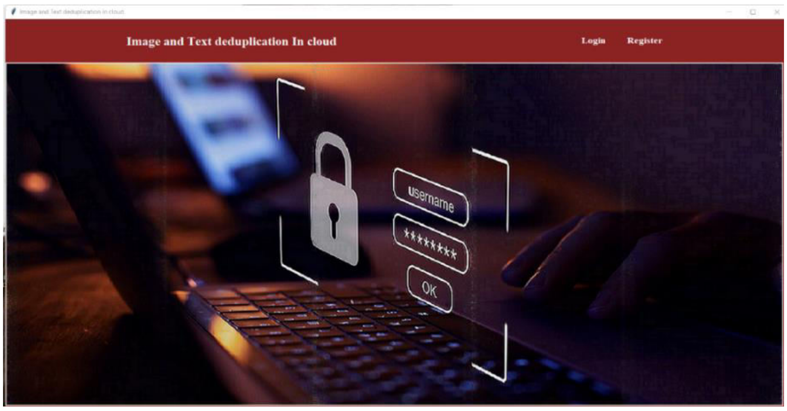
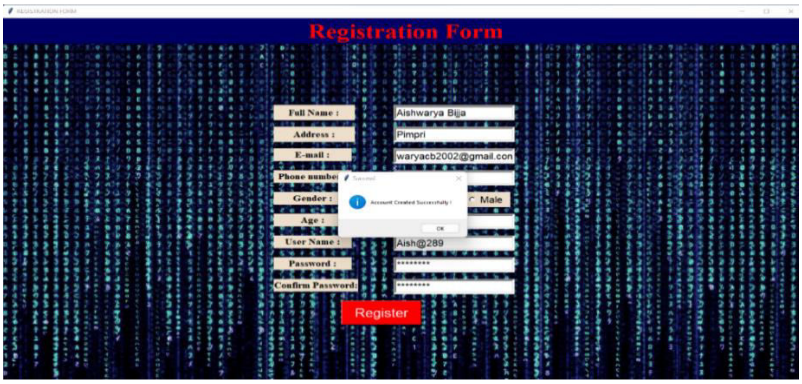


Image and Text deduplication In cloud

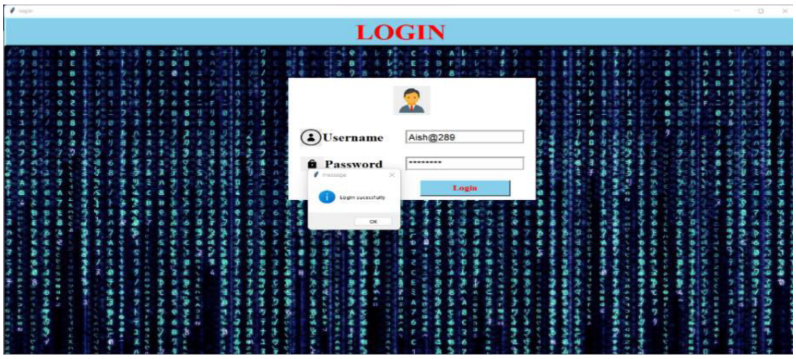
Fig 4.1 Home Page


Registration Form

Full Name :	Aishwarya Bijja
Address :	Pimpri
E-mail :	waryacb2002@gmail.con
Phone numbe	
Gender :	○ Male
Age :	
User Name :	Aish@289
Password :	********
Confirm Password:	********

Account Created Successfully !

Fig 4.2 Registration Page

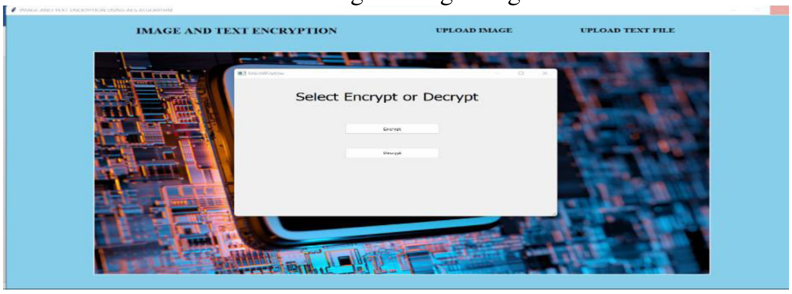


Username Aish@289

Password *********

Login sucessfully

Fig 4.3 Login Page



Select Encrypt or Decrypt

Fig 4.4 Encryption and Decryption

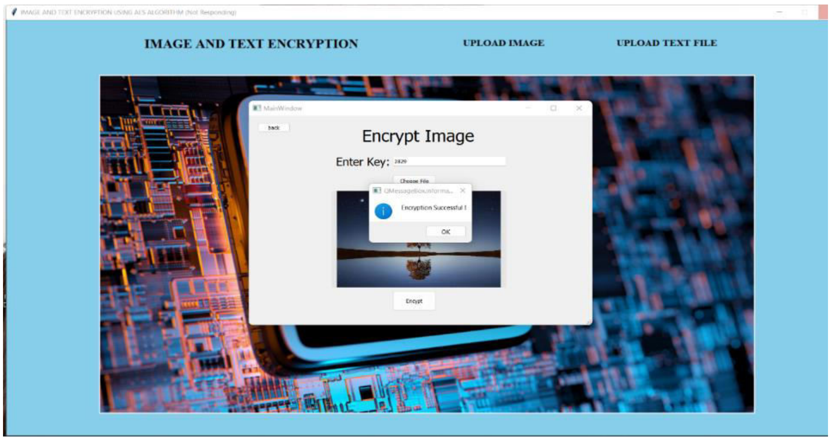


IMAGE AND TEXT ENCRYPTION USING AES ALGORITHM (Not Responding)
IMAGE AND TEXT ENCRYPTION
UPLOAD IMAGE
UPLOAD TEXT FILE
MainWindow
back
Choose File
QMessageBox.informa...
OK
Encypt

Encrypt Image

Enter Key: 2829

Encryption Successful !

Fig 4.5 Image Encryption

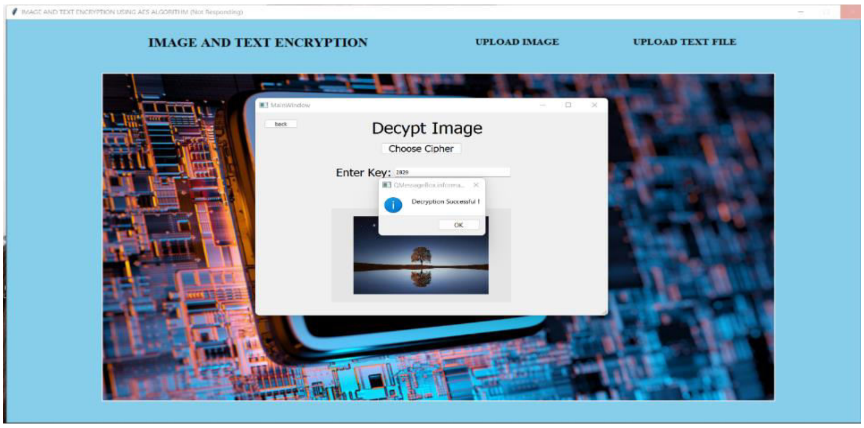


IMAGE AND TEXT ENCRYPTION USING AES ALGORITHM (Not Responding)
IMAGE AND TEXT ENCRYPTION
UPLOAD IMAGE
UPLOAD TEXT FILE
MainWindow
back
Choose Cipher
QMessageBox.informa...
OK

Decypt Image

Enter Key: 2829

Decryption Successful !

Fig 4.6 Image Decryption

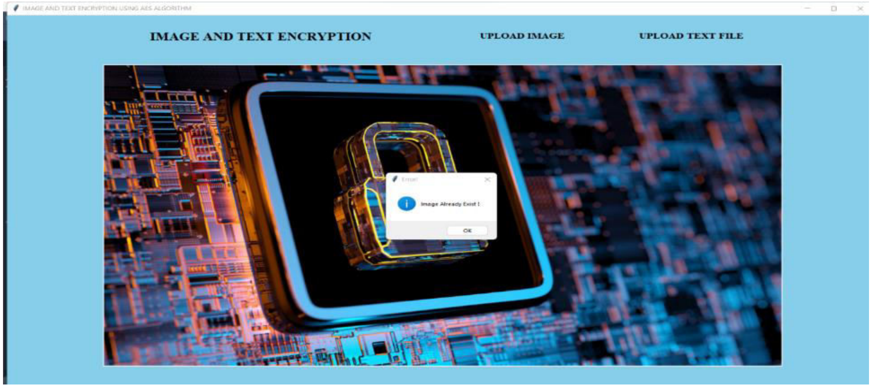


IMAGE AND TEXT ENCRYPTION USING AES ALGORITHM
IMAGE AND TEXT ENCRYPTION
UPLOAD IMAGE
UPLOAD TEXT FILE
Error
OK

Image Already Exist !

Fig 4.7 Image Deduplication Success

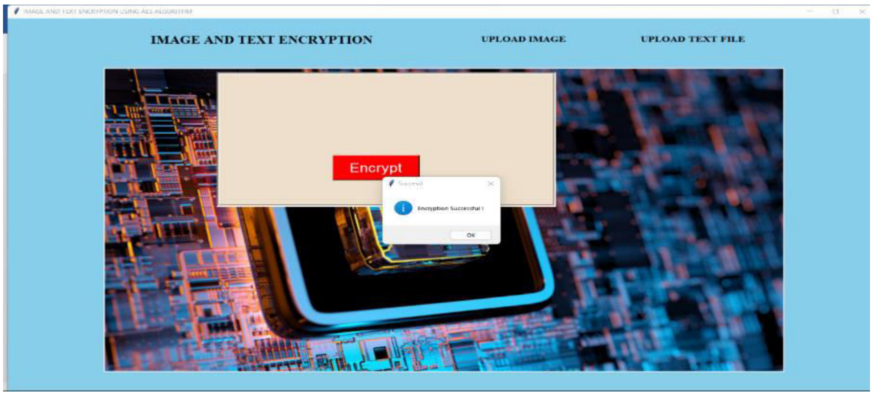


IMAGE AND TEXT ENCRYPTION USING AES ALGORITHM
IMAGE AND TEXT ENCRYPTION
UPLOAD IMAGE
UPLOAD TEXT FILE
Encrypt
Success
OK

Encryption Successful !

Fig 4.8 Text Encryption

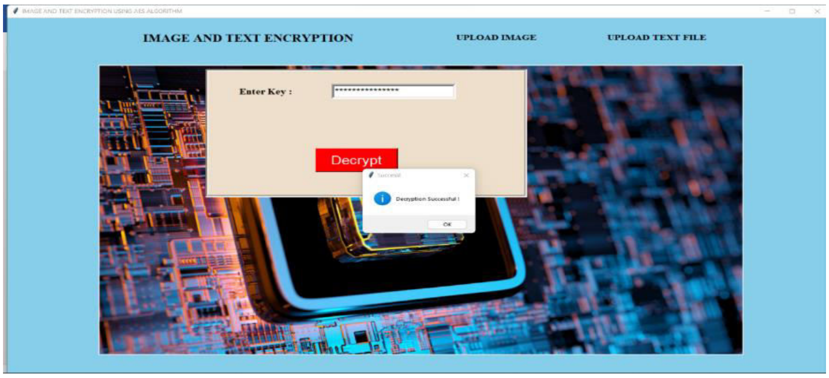
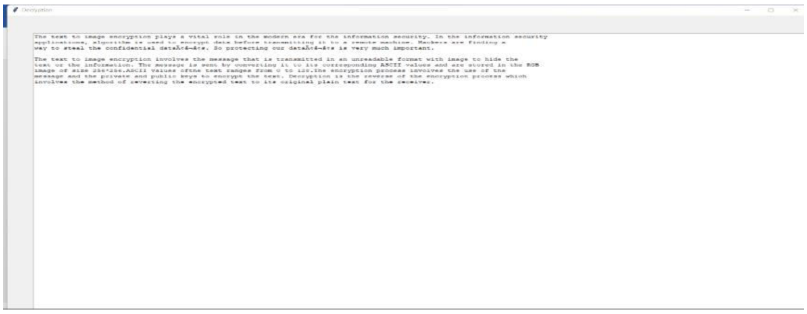


IMAGE AND TEXT ENCRYPTION USING AES ALGORITHM
IMAGE AND TEXT ENCRYPTION
UPLOAD IMAGE
UPLOAD TEXT FILE
Decrypt
Success
OK

Enter Key : ***************

Decryption Successful !

Fig 4.10 Text Decryption



```
The text to image encryption plays a vital role in the modern era for the information security. In the information security
applications, algorithm is used to encrypt data before transmitting it to a remote machine. Hackers are finding a
way to steal the confidential dataÃ¢â¬â¢s. So protecting our dataÃ¢â¬â¢s is very much important.

The text to image encryption involves the message that is transmitted in an unreadable format with image to hide the
text or the information. The message is sent by converting it to its corresponding ASCII values and are stored in the RGB
image of size 256*256.ASCII values ofthe text ranges from 0 to 128.The encryption process involves the use of the
message and the private and public keys to encrypt the text. Decryption is the reverse of the encryption process which
involves the method of reverting the encrypted text to its original plain text for the receiver.
```

Fig 4.11 Decrypted Text

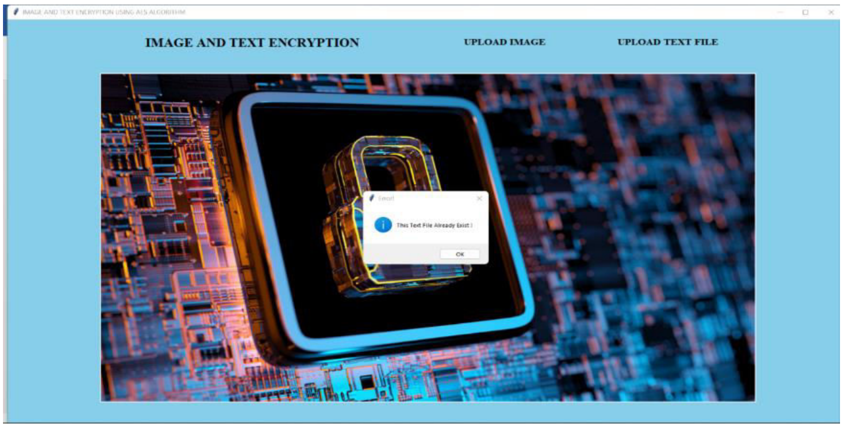


IMAGE AND TEXT ENCRYPTION USING AES ALGORITHM
IMAGE AND TEXT ENCRYPTION
UPLOAD IMAGE
UPLOAD TEXT FILE
OK

This Text File Already Exist !

Fig 4.12 Text Deduplication Sucess

IV. FUTURE SCOPE

Data deduplication, an efficient approach to data reduction, has gained increasing attention and popularity in large-scale storage systems due to the explosive growth of digital data.

It eliminates redundant data at the file or subfile level and identifies duplicate content by its cryptographically secure hash signature which is shown to be much more computationally efficient than the traditional compression approaches in large-scale storage systems.

V. CONCLUSION

In this survey, we have learned to prevent duplication using the Encryption and decryption methods. Many deduplication methods are already present, but they provide low security. For the text uploading we are supposed to analyse two algorithms, The uploading in the cloud system we will be using the Structural Similarities AES Algorithm the main goal of the similarity index is to recognize and check the image's quality such as pixels, radiance, contradiction and the structure of image, afterwards, it measures the similarity in the two images. To reserve a large amount of data with its efficiency, and to prevent duplicate texts and images we are using the method of encryption.

De-duplication of data, is an extremely efficient technique for data reduction, advantageous or beneficial attention. This has been accepted to be more efficient than traditional compression methods on huge data storage systems.

The outcome of the study display that the proposed solution can significantly reduce storage costs by removing and altering duplicate data, while also providing strong data security through encryption and access control. The study also highlights the main importance of authorized deduplication in ensuring that data is not accidentally deleted or modified by unauthorized users.

REFERENCES

[1] Nayan Panpatil, Madhavi Birla, Pragati Aher "Data security using cryptography with image and text deduplication in cloud" International journal of Scientific Development and Research 2022.
[2] Kanika.S.Gandhi, Devshree.S.PatekaR "Data Deduplication with encryption in cloud"International Journal of Innovative research in Science, Engineering and technology 2019.
[3] Pokala Phanitej, Y.Suresh "Encrypted data Management with deduplication in cloud computing"International Journal of Advance Research 2454-132X/2018.
[4] Mukhid Lashkari, Siddheshwar, Shubham Kathale "Deduplication of encrypted Textual data in cloud environment" International Journal of Research in Engineering 2581-5792/2019.
[5] Rashmi Singh, Shristi Priya "Deduplication in Cloud Computing" Journal of EmergingTechnologies and innovative Research 2349-5162/2018.

[6] M.Maharasi, S.Keerthiga, P.Kiruthika "Removal of dupliacte storage of encrypted data in cloud computing Environment" International Journal of Engineering Research in computer science and engineering 2391-2320/2018.

[7] Ali Miri , Fatema Rashia "Secure Textual Data Deduplication Scheme Based on Data Encoding and compression" IEEE 2019.

[8] Ali.A.Ghorbhani, Xue Yang "Achieving Efficient and Preserving Multidomain Big Data Deduplication in cloud" IEEE Transaction on service computing 10.1109/TSC 2018.2881147.

[9] S.Uthayashanagr, J.Abinaya, V.Harshini "Image and Text Encrypted with AuthorizedDeduplication in cloud" IEEE 2020

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com