AWS based-Secure File Storage Using Hybrid Cryptography

CLOUD COMPUTING COURSE PROJECT REPORT

Submitted by

Group No.-19

M Sai Hemant
211000029

Shriniwas Raju Jagadabhi
211000053

Sontu Akshath Rishi
211000057

Vidapu Bhanu Teja
211000060

Under the guidance of
Dr Kavita Jaiswal
(Assistant Professor, IIITNR)

Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur

Abstract

The adoption of cloud computing has transformed the way we store and manage our data. With the convenience and scalability of cloud storage, increased businesses and individuals are entrusting their sensitive information to third-party cloud providers. However, with this convenience comes the risk of security breaches, data loss, and unauthorized access.

The importance of secure file storage in the cloud cannot be overstated. Cloud providers store data from multiple clients on shared infrastructure, making it vulnerable to cyber-attacks and data breaches. This means that sensitive data such as financial records, health records, and personal information are at risk of exposure to unauthorized third parties. The consequences of a security breach can be catastrophic, including monetary loss, legal liabilities, and damage to the reputation of the affected organization. To mitigate the risks associated with cloud storage, cryptography plays a crucial role in ensuring data confidentiality, integrity, and availability. Cryptography uses mathematical algorithms to encrypt and decrypt data, making it unreadable to unauthorized parties. This ensures that only authorized parties can access and modify the data, even if it falls into the wrong hands. To further enhance cloud security, various measures can be implemented, such as access control, data backups, disaster recovery plans, and regular security audits. Access control ensures that only authorized users can access the data, while backups and disaster recovery plans protect against data loss and ensure business continuity in the event of a security breach. Regular security audits help to identify and address vulnerabilities before they can be exploited by cybercriminals.

Introduction

The use of technology in our daily lives has increased tremendously, leading to an increase in online data storage. However, protecting online data has become a significant problem. Cryptography can be used to secure data, especially in cloud-based storage, where poor protection can lead to security breaches. Cloud-based internet security is a viable solution to enhance user security.

The dynamic scalability and multi-tenant nature of cloud computing make standard security procedures inadequate. Hybrid encryption, which combines symmetric and asymmetric encryption, is a secure method to protect cloud storage infrastructure. RSA and AES algorithms are used to demonstrate the differences between less secure and more secure systems.

One way to secure file data in AWS cloud is by encrypting the entire format, not just the content. Steganography can also be used to embed the key in an image before sending it as an email attachment, providing an added layer of security.

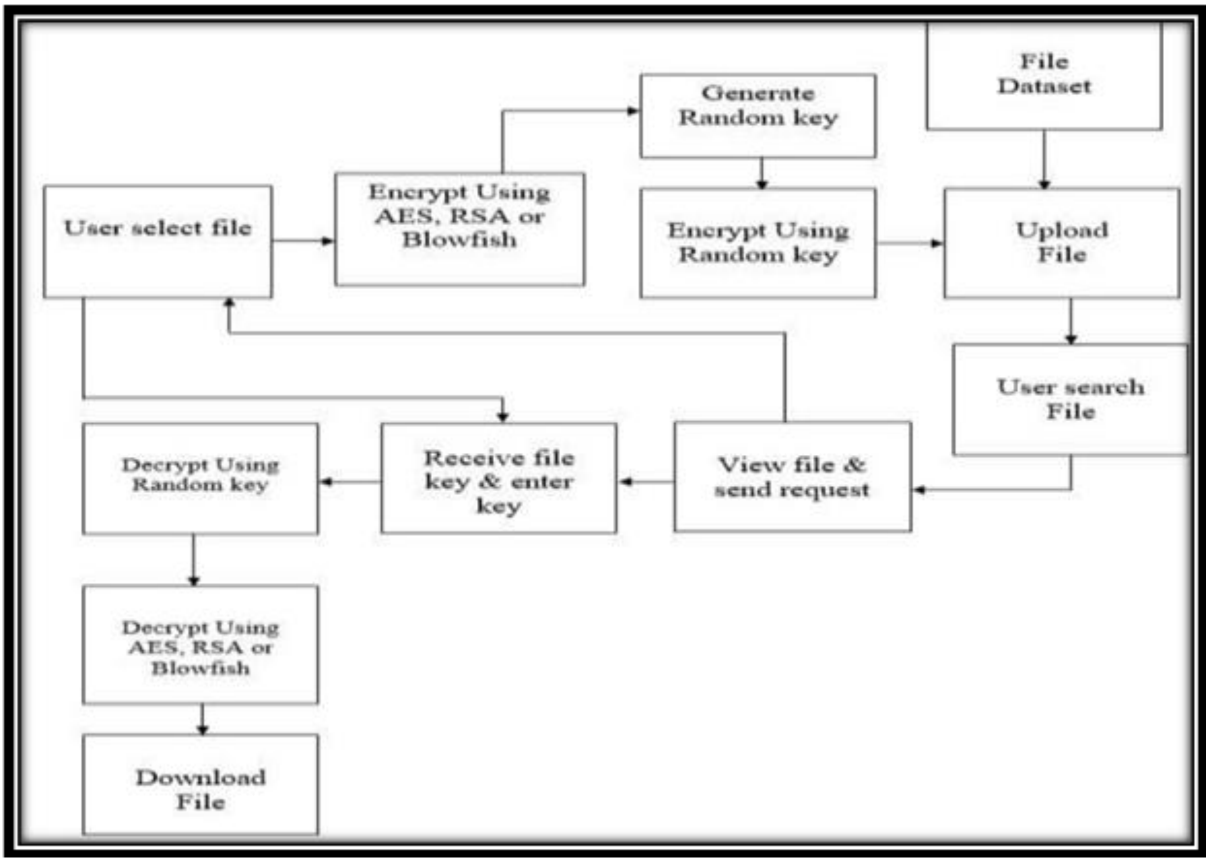
Background

The need for secure file storage has become increasingly important as more individuals and organizations move their data to the cloud. While cloud-based storage offers several benefits, such as scalability and accessibility, it also poses significant security risks. Cyberattacks, data breaches, and unauthorized access can result in the loss of sensitive information, and in some cases, legal and financial implications.

Hybrid encryption is a technique that combines symmetric and asymmetric encryption to provide both speed and security benefits. This method is highly secure if the public and private keys are secure. It can be used to protect cloud storage infrastructure, and the RSA and AES algorithms can be employed to demonstrate the differences between secure and insecure systems. The RSA algorithm is used to encrypt the key, while the AES algorithm is used to encrypt text or data.

To ensure secured file data in the AWS cloud, the file's entire format can be encrypted, not just the content. Additionally, steganography can be used to embed the key in an image and send it as an email attachment, providing an additional layer of encryption.

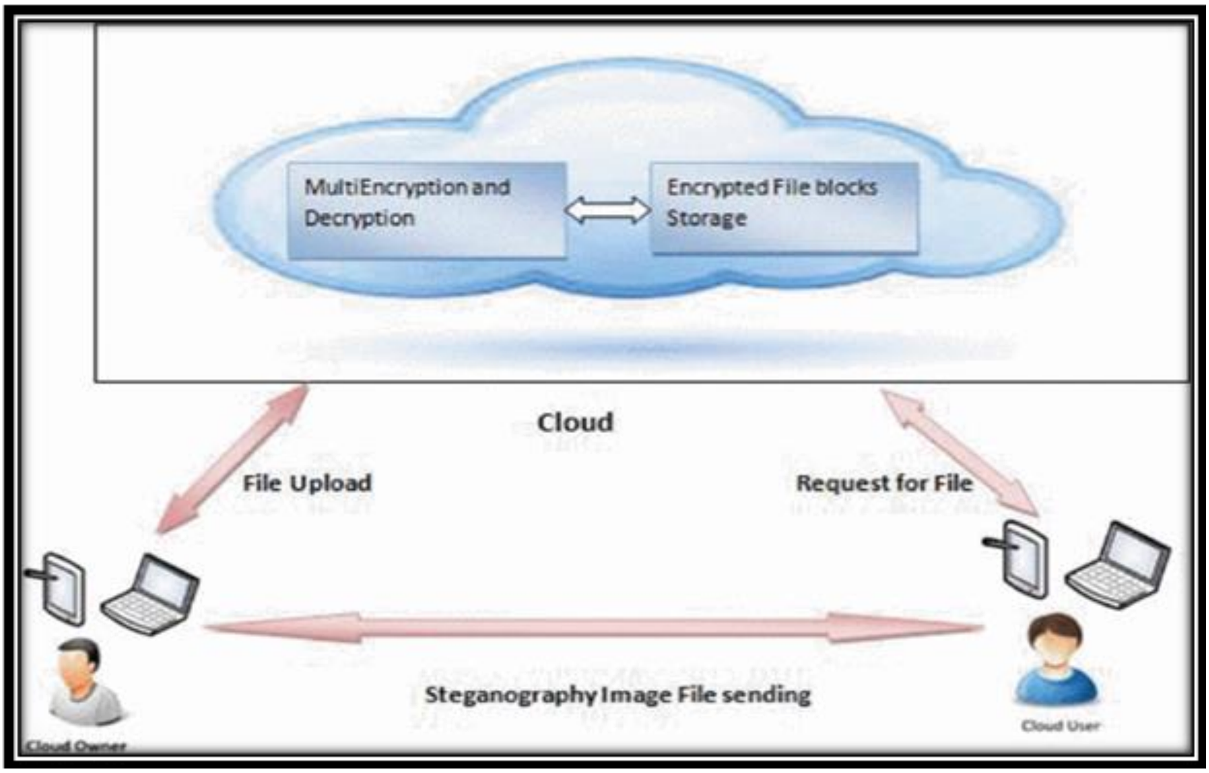
Architecture



System Model

Hybrid encryption is a straightforward concept. We encrypt the message with AES rather than using it to encrypt the text. The key is then kept secret by them, and we use RSA to encrypt it. The steps below are followed to achieve our main objective of our project. The first stage is to create a symmetric key, which must be kept secret. The second step is to use the secret symmetric key to encrypt the data. The recipient of our communication will now disclose their public key with us, but we must keep their private key a secret. We now need to use the receiver's public key to encrypt the symmetric key. The text of the encrypted message must be sent. The recipient obtains the symmetric key required for decryption by using their private key to decrypt the encrypted symmetric key. The receiver now decrypts the message using the decrypted symmetric key to obtain the original message.

You must first set up your AWS account and build a bucket to configure AWS S3 for uploading and fetching files from the bucket. IAM users should be set up, and access should be granted either through a bucket policy or at the user level. You can quickly specify which paths users can update and access with bucket policies. You can create an IAM user for Programmatic (CLI) access exclusively, which will offer you a unique set of credentials when you establish an IAM user. Simply configure the access and token keys using AWS. Additionally, you should check to see if you are creating an IAM user for yourself, as this is often advised for security. To do this, go to AWS Access Key and select "Create New Access Key" under the Access keys (access key ID and secret access key) section. Additionally, do not forget to write down the AWS Secret Access Key because it is a one-time use item that cannot be recovered if lost or forgotten.

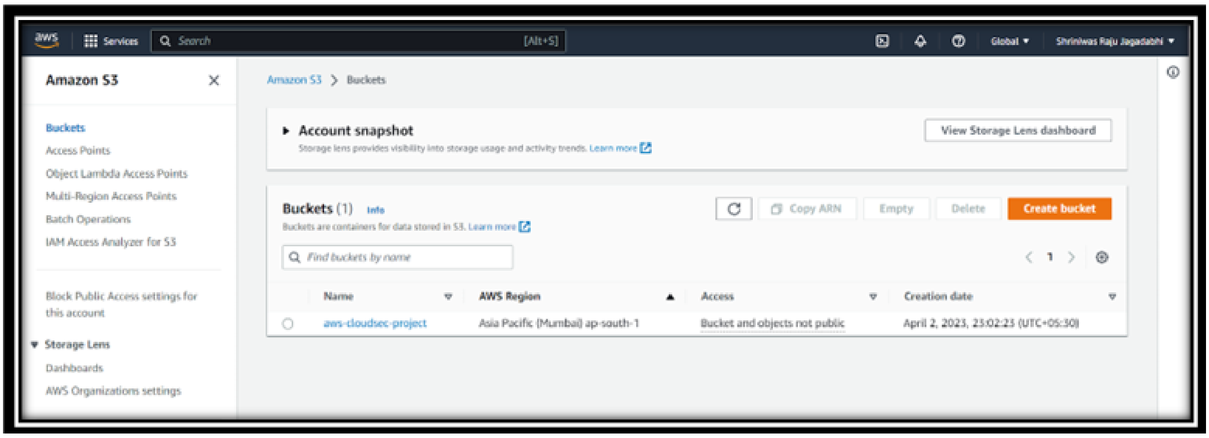

MultiEncryption and Decryption
Encrypted File blocks Storage
Cloud
File Upload
Request for File
Steganography Image File sending
Cloud Owner
Cloud User

Instead, you must generate a fresh access key and deactivate the old one. Open Windows cmd and type after writing down the credentials: aws configure. Using your Mailtrap account is necessary for the decryption stage of this procedure. You must create a Mailtrap account. To utilize Mailtrap's API after joining up, you simply need to have your login and password on hand. The SMPT settings option is where you can find the smtp login information. Running this Python script after modifying will create a configurations.ini file in the same directory that you can use to quickly customize the software.

Cloud Technology

The cloud platform used for this project is AWS.

Amazon Web Services, Inc. (AWS) is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis. Oftentimes, clients will use this in combination with autoscaling (a process that allows a client to use more computers in times of high application usage, and then scale down to reduce costs when there is less traffic). These cloud computing web services provide assorted services related to networking, computing, storage, middleware, IOT and other processing capacity, as well as software tools via AWS server farms. AWS services are delivered to customers via a network of AWS server farms worldwide.



Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets are containers for data stored in S3. Learn more

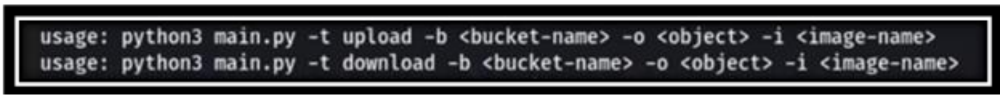
	Name	AWS Region	Access	Creation date
○	aws-cloudsec-project	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	April 2, 2023, 23:02:23 (UTC+05:30)

For this project, the cloud is used as a platform as a service (PaaS).

One of the most significant benefits of cloud computing is its ability to provide platform as a service (PaaS) solutions to businesses. PaaS allows businesses to develop, deploy, and manage their applications and services in the cloud, without the need to invest in the underlying infrastructure. Paas provides a complete development and deployment environment in the cloud, which includes development tools, application servers, databases, and operating systems. Cloud-based PaaS solutions also offer scalability and flexibility. Businesses can easily scale up or down their application resources based on demand, without worrying about the underlying infrastructure. This enables businesses to respond quickly to changing business needs and reduces the cost of maintaining infrastructure. However, with the increasing use of cloud-based PaaS solutions, the security of data stored in the cloud has become a major concern for businesses. The security of data in the cloud is crucial because it is vulnerable to attacks from hackers and cybercriminals.

Results

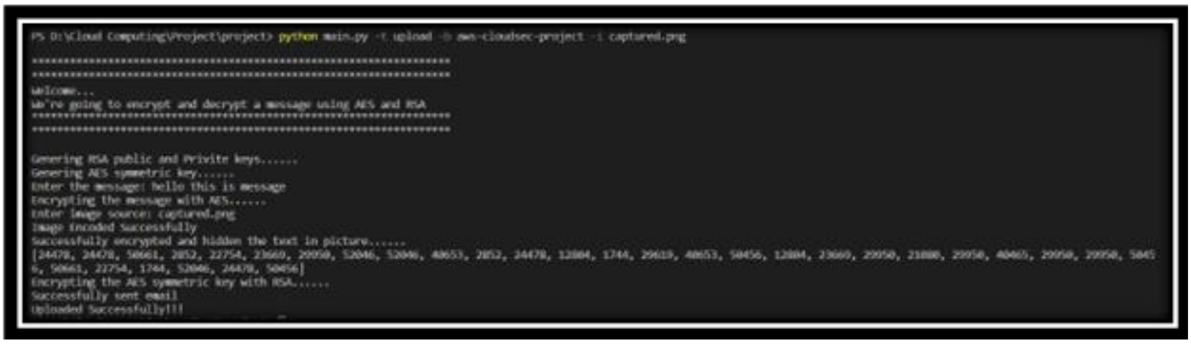
To configure AWS S3 to upload and download files from the bucket, you must first create a bucket and set up your AWS account. After doing that you have to give these commands to do the following operation



```
usage: python3 main.py -t upload -b <bucket-name> -o <object> -i <image-name>
usage: python3 main.py -t download -b <bucket-name> -o <object> -i <image-name>
```

Fig 1: Commands to Configure AWSs3 To Upload and Download Files

Now it was generating RSA public and private keys and generating AES symmetric key now there will be input taken enter the message the message given was “hello this is message “.Now this message was encrypted with AES the image source was captured.png now this image is encoded successfully and it was successfully encrypted and hidden the text in picture .After that Encrypting the AES symmetric key with RSA the email is successfully sent and uploaded



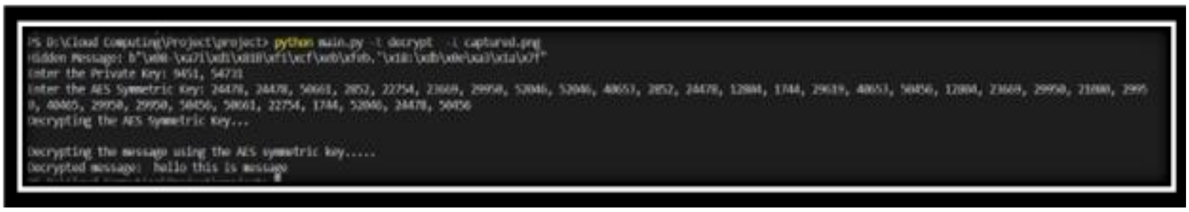
```
PS D:\Cloud Computing\Project\project> python main.py -t upload -b aws-cloudsec-project -i captured.png

****************************************************************
****************************************************************
Welcome...
We're going to encrypt and decrypt a message using AES and RSA
****************************************************************
****************************************************************

Genering RSA public and Privite keys......
Genering AES symmetric key......
Enter the message: hello this is message
Encrypting the message with AES......
Enter image source: captured.png
Image Encoded Successfully
Successfully encrypted and hidden the text in picture......
[24478, 24478, 50661, 2852, 22754, 23669, 29950, 52046, 52046, 40653, 2852, 24478, 12884, 1744, 29619, 40653, 50456, 12884, 23669, 29950, 21880, 29950, 40465, 29950, 29950, 5045
6, 50661, 22754, 1744, 52046, 24478, 50456]
Encrypting the AES symmetric key with RSA......
Successfully sent email
Uploaded Successfully!!!
```

Fig 2: Encryption of Message and Png Encoding

We can see the hidden message in hash form. After that we need to give the private key and AES symmetric key which was sent to the email. After that the decryption of AES symmetric key was done after that we can clearly see the decrypted text message.

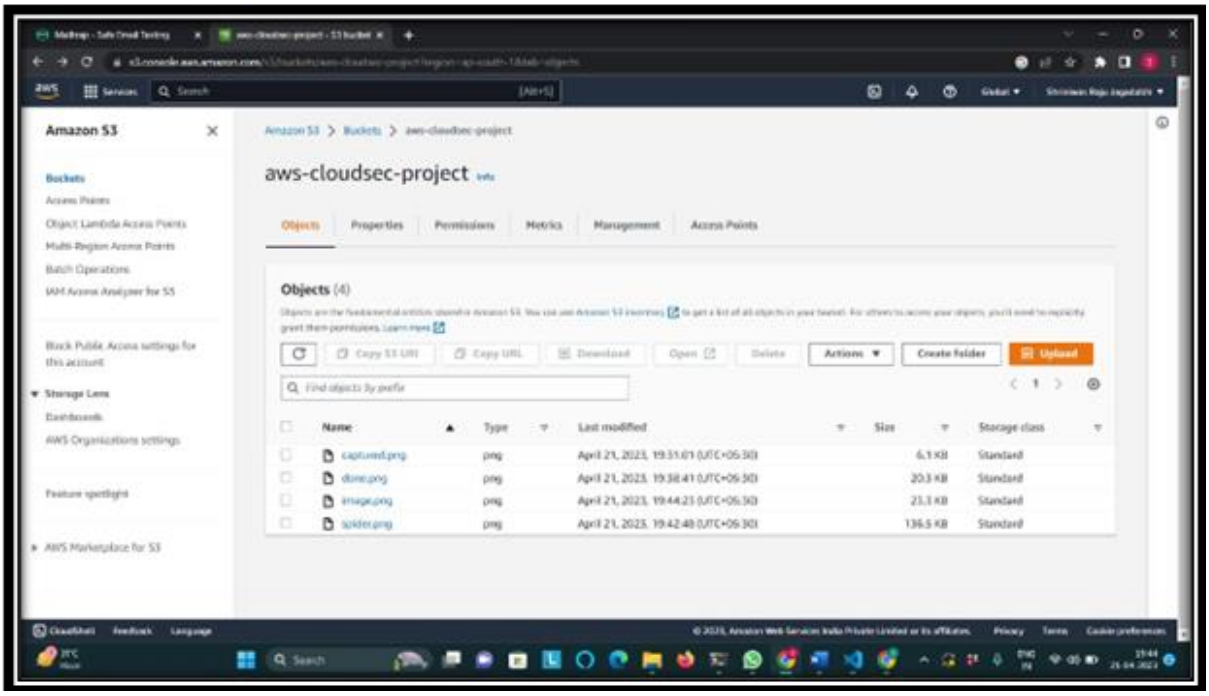


```
PS D:\Cloud Computing\Project\project> python main.py -t decrypt  -i captured.png
Hidden Message: b"\x08-\xa71\xd1\x818\xf1\xcf\xeb\xfeb.'\xd8:\xdb\x0e\xa3\xda\x7f"
Enter the Private Key: 9451, 54731
Enter the AES Symmetric Key: 24478, 24478, 50661, 2852, 22754, 23669, 29950, 52046, 52046, 40653, 2852, 24478, 12884, 1744, 29619, 40653, 50456, 12884, 23669, 29950, 21880, 2995
0, 40465, 29950, 29950, 50456, 50661, 22754, 1744, 52046, 24478, 50456
Decrypting the AES Symmetric Key...

Decrypting the message using the AES symmetric key.....
Decrypted message:  hello this is message
```

Fig 3: Decrypted Message

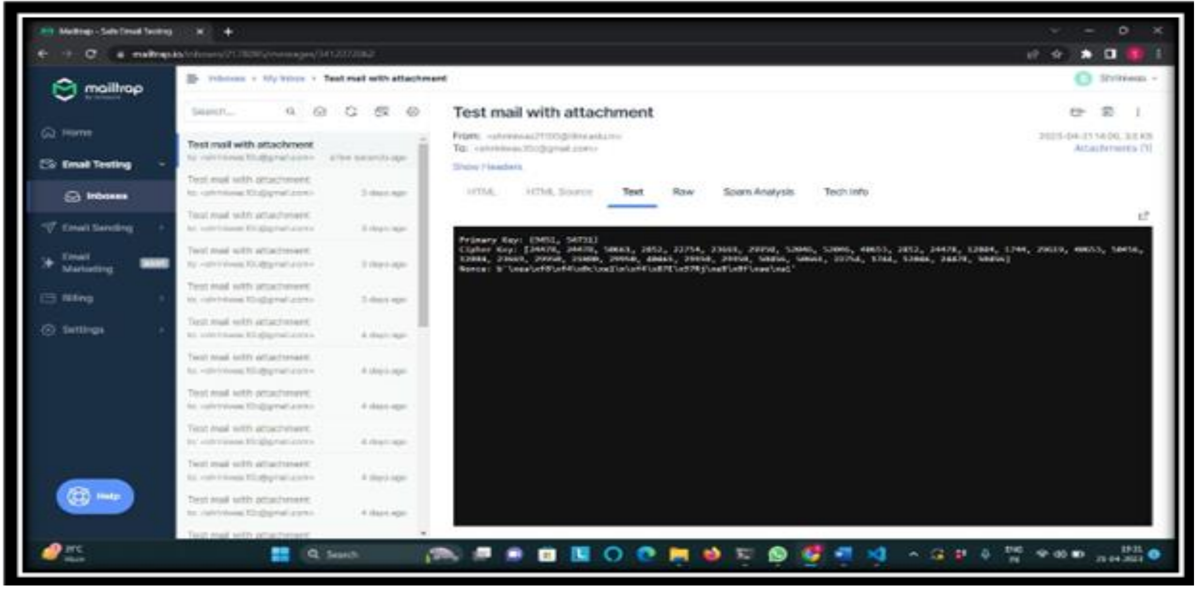
As we can see in AWSs3 the buckets are created and the files are uploaded and downloaded, respectively.



Name	Type	Last modified	Size	Storage class
captured.png	png	April 21, 2023, 19:31:01 (UTC+05:30)	6.1 KB	Standard
done.png	png	April 21, 2023, 19:38:41 (UTC+05:30)	20.3 KB	Standard
image.png	png	April 21, 2023, 19:44:23 (UTC+05:30)	23.3 KB	Standard
spider.png	png	April 21, 2023, 19:42:48 (UTC+05:30)	136.5 KB	Standard

Fig 4: Files and AWS Cloud Storage

The test email can be seen here, and the private keys are sent to mail



```
Primary Key: [illegible]
Cipher Key: [illegible]
Nonce: b'[illegible]'
```

Conclusion

The use of hybrid cryptography in AWS-based secure file storage is an effective solution to protect sensitive information from unauthorized access. This technique provides both speed and security benefits and ensures that files stored in the cloud are highly secure. This system's major objective is to safely store and retrieve data from the cloud that is only accessible to the data's owner. Cryptography and steganography techniques are used to address the data security challenges associated with cloud storage. RSA and the AES algorithm are used to secure data. The LSB method securely stores important data (Steganography). Using multithreading technology, the encryption and decryption procedure takes less time. We have improved data integrity, high security, low delay, authentication, and confidentiality with the proposed security method. With the increasing importance of secure file storage, the use of hybrid cryptography in AWS provides a highly secure and efficient method for storing and sharing sensitive information.Public key cryptography can be added in the future to prevent assaults on the data transmission from the client to the server.