International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 04, 2023
www.ijirse.com
ISSN: 2454-9665

Private Document Vault with server sideEncryption Using Cloud AWS

Ch.Purna Lokesh Reddy, D.Apoorva, Sk. Jaleel Basha, G. Manikanta, N. Purna Chandarao, Mr. M. Ambarisha

Department ofInformation Technology, Tirumala Engineering College

ABSTRACT

With the evolution of computer systems, the amount of sensitive data to be stored as well as the number of threats on these data grows up, making data confidentiality increasingly important to computer users.

A simple solution is for the user to encrypt all documents before submitting them. This method, however, makes it impossible to efficiently search for documents as they are all encrypted. We propose a private document vault with server side encryption, which also enables customers to easily deploy encryption and other security solutions by offering robust, central management of encryption keys In addition, this paper designs and implements a prototype system. Through the verification and analysis of its usability and security, it is proved that the solution can meet the data security protection requirements of sensitive Edocuments in the open network environment.

I. INTRODUCTION

Encryption is one of the most basic requirements for ensuringdata privacy, especially for end-to-end protection of data transmitted across networks. Plaintext is encrypted using an encryption algorithm and an encryption key. Encryption converts the readable text to an unreadable text which is called cipher text (encrypted data). Server-side encryption is the encryption of data at its destination by the application or service that receives it. Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. If you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a resigned URL, that URL works the same way for both encrypted and unencrypted objects. Additionally, when you list objects in your bucket, the list API returns a list of all objects, regardless of whether they are encrypted.

II. Server Side Encryption

S3 Server-Side Encryption

- Server-side encryption is about data encryption at rest
- Server-side encryption encrypts only the object data.
- Any object metadata is not encrypted.
- S3 handles the encryption (as it writes to disks) anddecryption (when objects are accessed) of the data objects

ISSN: 2454-9665

In Server-side encryption, the data is encrypted after being sent to the S3 bucket and before storing it in the S3 bucket. Server-side encryption has the following three options:

1. **Use Amazon S3-managed keys (SSE-S3): -** In this, the keymaterial and the key will be provided by AWS itself to encryptthe objects in the S3 bucket.

2. **Use CMK (Customer Master key) in AWS KMS (SSE-KMS): -** In this, key material and the key will be generated in AWS KMS service to encrypt the objects in S3 bucket.

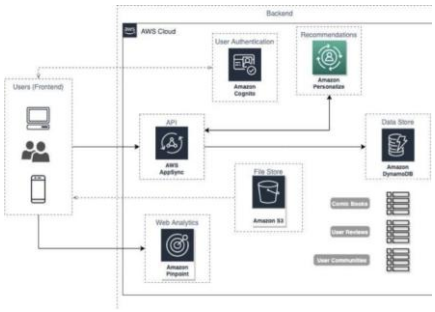
3. **Use a customer provided encryption key (SSE-C): -** In this, the key will be provided by the customer and Amazon S3 manages the encryption and decryption process while uploading/downloading the objects into the S3 bucket.

III. LITERATURE SURVEY

I Made Ari Dwi Suta Atmaja, I Nyoman Gede Arya Astawa, Ni Wayan Wisswani, I Made Riyan Adi Nugroho, "Document Encryption Through Asymmetric RSA Cryptography", International Conference on Applied Science and Technology (iCAST), 2021 Cryptography is one method for securing digital documents and data. The most secure data security technique is asymmetric key cryptography. The RSA (Rivest-Shamir-Adleman) algorithm is one of the most widely used asymmetric cryptography algorithms. The most frequently attached document when sending e-mails is an encrypted document. The document formats are.docx,.pptx,.xlsx,.pdf,.jpg, and.mp4. A public key and a private key will be generated during the encryption process and can be sent individually by sending encrypted digital documents. The decryption of digital documents is performed from the receiving end of the file using a private key generated during the encryption process. The encrypted file is larger in size than the original file. Because it has been encoded in a different manner using the RSA algorithm. The longer and larger the input size, the longer it will take for encryption to complete. These are analysed based on the cell parameters like cell size, the area, width, colour etc. These are very peculiar and not exactly known to user unless by performing some calculations.

IV. PROPOSED SYSTEM:

Fig: Proposed System



The most complete and widely used cloud platform in the world, Amazon Web Services (AWS), provides over 200 fully functional services from data centers across the world. Millions of clients use AWS to save costs, increase agility, and accelerate innovation, including the largest corporations, most successful governmental

ISSN: 2454-9665

organizations, and the fastest growing startups. Compared to other cloud providers, AWS offers a significantly greater number of services and features within those services, ranging from infrastructure technologies like compute, storage, and databases to cutting edge technologies like artificial intelligence, machine learning, data lakes, and the Internet of Things. As a result, moving your current applications to the cloud is quicker, simpler, and more cost-effective, and you can construct almost anything you can think of. AWS provides the most comprehensive functionality among such services. For instance, AWS has the greatest selection of databases that arecreated specifically for certain applications, allowing you to select the finest tool for the task at the best price and performance.

V. ARCHITECTURE OF PROPOSED SYSTEM

There are two types of algorithms are used

1. FERNET Fernet algorithm guarantees that a message encrypted using it cannot be manipulated or read without the key. Fernet is an implementation of symmetric (also known as “secret key”) authenticated cryptography
2. RSA RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

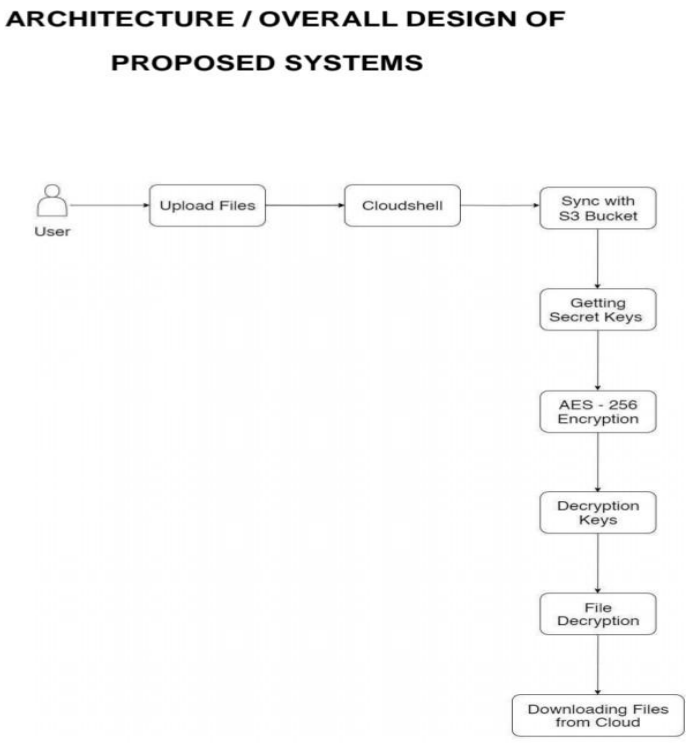
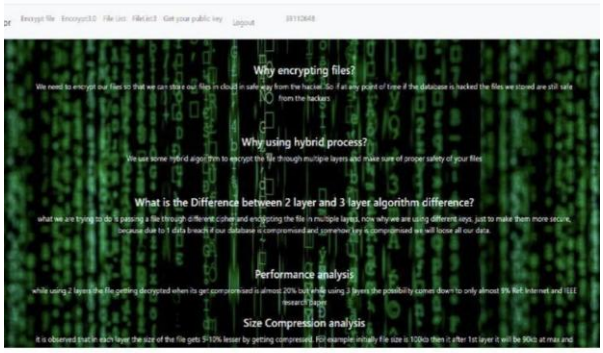


Fig 4.2: System Architecture

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 04, 2023
www.ijirse.com
ISSN: 2454-9665

VI. RESULTS



CONCLUSION

This project is designed to Encrypt the files in the using the cloud server AWS S3 Bucket and the encryption algorithm used are RSA and Fernet which can be used \to encrypt the files using 2 tier or 3 tier encryption .By this project more data can encrypted easily using cloud server of AWS

REFERENCES

[1] I Made Ari Dwi Suta Atmaja, I Nyoman Gede Arya Astawa, Ni Wayan Wisswani, I Made Riyan Adi Nugroho, "Document Encryption Through Asymmetric RSA Cryptography", International Conference on Applied Science and Technology (iCAST), 2021

[2] Yuxiang Lin, Xin Xia, Jingyi Yang, "Document Encryption Method with Mechanism of Enigma Machine", International Conference on Artificial Intelligence, Big Data and Algorithms(CAIBDA), 2021

[3] S. D. Sanap, Vijayshree More, "Analysis of Encryption Techniques for Secure Communication", International Conference on Emerging Smart Computing and Informatics (ESCI), 2021

[4] Alpana A. Ingale, Sunil K. Moon, "E-Government Documents Authentication and Security by Utilizing Video CryptoSteganography", IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2019

[5] Bryan H. Wodi, Carson K. Leung, Alfredo Cuzzocrea, S. Sourav, "Fast Privacy-Preserving Keyword Search on Encrypted Outsourced Data", IEEE International Conferenceon Big Data (Big Data), 2020