Secure File Sharing System Using Encryption and Decryption Algorithm

HAMDA NAVISH[1], VARTIKA LOHAT[2], SUMEDHA BHARDAWAJ[3]
[1, 2] *Student, School of Computing, DIT University, Dehradun, Uttarakhand*
[3] *Assistant Professor, School of Computing, DIT University, Dehradun, Uttarakhand*

Abstract*— This paper focuses on securely storing information within cloud systems, emphasizing confidentiality and integrity. In today's data- driven world, ensuring robust security measures is essential for seamless sharing and transfer of files. Cloud computing offers a shared network infrastructure, enabling convenient access to data across various devices. Users can share files and store data in colocation data centres, accessible on demand without direct server access. Security concerns are addressed using cryptographic techniques, including AES and DES algorithms, to restrict unauthorized access. The paper outlines the combination of these algorithms to safeguard user data, preventing unauthorized users from accessing private information. Security and privacy in developing an application tailored for securely sharing files over the cloud, employing user authentication to enhance data protection has been prioritized.

Index Terms – Cryptographic techniques, Cloud Computing, AES, DES.

I. INTRODUCTION

In today's world of connections, the need to secure file sharing has become paramount. Whether the data is sensitive documents, personal data, or confidential information, With the increase in cyber threats and the increase in cyber criminals, sharing file methods are insufficient for providing sufficient protection from cyber criminals and their unauthorized attacks.

To address these challenges, the development of secure file sharing using encryption and decryption algorithms turns out to be a solution. By applying these cryptographic techniques, it is certain that the user's data can be secured from unauthorized access. The data should be uploaded to the cloud in such a form that even if the security of the cloud is compromised, the data is not readable to the attacker. Cryptography is a technique to protect data from unknown users. It is aimed at safeguarding data from unauthorized access, encompasses two primary types of algorithms: symmetric key algorithms, also called conventional key algorithms, and asymmetric key algorithms, occasionally referred to as public-key algorithms, each serving distinct cryptographic purposes. [1] CLOUD (Communities and Libraries Online Union Database) is a platform where the data of users is stored, and they can remotely access it anywhere and anytime they wish to.[8] Data storage is the basic service that is provided by the cloud. Cloud computing works on shared computer technology. It is an internet-based service. The growth of cloud computing is the result of growing demand for high-capacity networks, less expensive computers with high efficiency, and storage devices.

In cloud computing, security is a crucial aspect. It is because of the information that is being stored in the cloud. The data stored in the cloud is confidential and sensitive. Hence, the management of that data needs to be completely reliable. It is a necessity that the stored data be immune to malicious attacks. [11][13][14]

Figure 1: Cloud Storage

Therefore, it's all about keeping data private and making sure it doesn't get changed without permission. If data gets into the wrong hands, that's a privacy issue. Due to the failure of cloud services, data integrity also suffers.[1][2]

The Advanced Encryption Standard (AES) is a variant of block cipher and is established in the year 2001 by the US National Institute of Standards and Technology (NIST) and developed by two Belgian cryptographers, John, and Vincent Rijmen.[1][4] This is a symmetric-encryption algorithm. AES works six times speedier than Data Encryption Standard (DES). AES is more powerful than DES because it has more power to prevent Brute Force Attacks. AES algorithms is widely used in diverse platforms which includes file encryption, Processor security and wireless security.

II. PROBLEM STATEMENT

Currently, secure file sharing is a necessity across various domains, such as government agencies, business, and personal communications. The data of user, which is being stored in the cloud, is vulnerable to various malicious attacks. A method to keep these threats away from the user's data and to provide protection from these threats is proposed in this study. The first threat is to data integrity. Data integrity means keeping data safe in the cloud, making sure it doesn't change without permission from the right people. It is the protection of data from intentional and accidental alterations without authorization. A user cannot completely rely on cloud service providers because they don't ensure full security of the user's crucial data. Therefore, there is an urgent need for the development of a secure file sharing system that uses advanced encryption and decryption algorithms to ensure two main aspects of security: integrity and confidentiality.

Prioritizing the resolution of key challenges such as encryption and decryption, the system implements robust algorithms to safeguard shared files confidentiality, guaranteeing that access is restricted to authorized users, all the while upholding usability and performance standards.

Security is a compulsory service to upgrade what is being offered in the cloud. Storing information in the cloud is not only about data availability; it is also about securely storing it. The point here is to generate a secret key to manage the security of data.[1]

The insufficiency of cloud storage to provide security is the main reason most businesses avoid using cloud services due to the fear of leakage of crucial data.[9][10] The cloud is a shared environment where resources are shared between multiple users, which can sometimes also include third-party services. This is because the data is always at higher risk of getting mishandled. There are also several external threats, one of which is data leakage, which includes malicious attacks by cloud providers and can also compromise the cloud user's account. Henceforth, the best solution and strategy is to use encryption and decryption algorithms, which include stronger passwords, and not only depend on cloud service providers.[13]

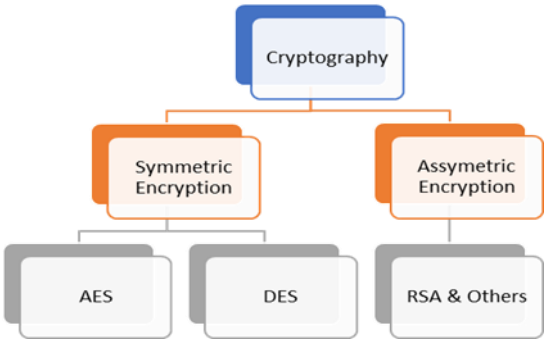

Figure 2: Types of Cryptography

III. CLASSIFICATION TECHNIQUES

a. Amazon Web Services (AWS):

A cloud computing platform known as AWS is offered by Amazon.com. It gives many kinds of services of cloud which includes storage solutions, database machine learning, etc. The main advantage of AWS is its infrastructure where various data centres are located intendedly around the globe to provide its customers with the convenience of deploying services closer to the end-users for faster access and better performance. AWS provides services and manages them with ease. The key strength of AWS lies in its infrastructure. AWS empowers organizations to deploy applications with ease and flexibility. It ensures that data of any size will be easy to store. AWS is preferred choice for businesses seeking scalable and cost-effective solutions for their computing needs.[2][6][7]

b. Symmetric-key cryptography:

The type of encryption technique where only one key used is known as symmetric key cryptography. In this encryption method a similar key is used to encrypt and

decrypt the file. Symmetric key encryption is the only known technique till June 1976.[1] This approach of encoding data has been in used in older times to deliver a secret message or used as a communication between government and militaries. Symmetric key ciphers are inexpensive because they can produce a strong key at a moderate rate and the algorithms are also inexpensive to procedure.

Block Ciphers and Stream Ciphers are two types of symmetric key ciphers. Stream Ciphers are a type of encryption technique which process in the form of bits, byte, or characters of plain text. Stream Cipher are usually faster than block ciphers. A block cipher encrypts plain text into cypher text by using a fixed size data block by using a shared key. The AES and DES are block ciphers.

c. Advanced Encryption Standard:

AES is an algorithm that uses a similar key to do encryption and decryption to protect the data. AES algorithms work as splitting the message into several smaller blocks. It is developed by Vincent Rijmen and Joan Daemen as a subset of Rijndael Cipher Development.

Rijndael is like a family of locks that come in different sizes and shapes, providing options for securing data in various ways. AES performs several rounds of substitution, transposition and mixing instead of just a single round of encryption. Each block of size is 128 bits in AES, but it has three different key lengths: 128, 192, and 256 bits. The 128-bit key undergoes 10 rounds of encryption, the 192-bit key undergoes 12 rounds of encryption, and the 256-bit key undergoes 14 rounds.[3][4]

The main aim of AES algorithm was to replace DES algorithm because DES algorithm is quite vulnerable to attacks. NIST invited people from all over the world to work on the encryption technique which is more efficient than DES. The experts from all over the world came and worked on encryption and data security to introduce an innovation block cypher algorithm to encrypt and decrypt data with more complex and powerful structure than DES.[4]

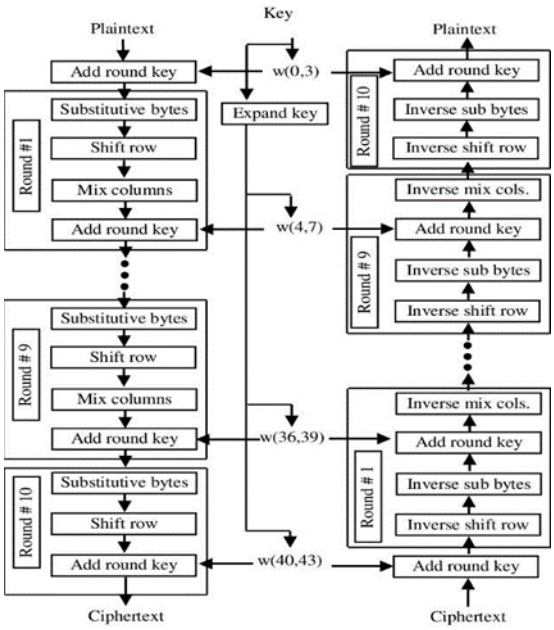

Figure 3: Encryption and Decryption Process

1. Byte Substitution:

As shown in figure 3 Byte Substitution is an important step in the development of AES, specifically in the substitution layer of algorithm.

This is also known as SubBytes. It works by swapping out each byte in the input block with a different byte using a special table called the S- Box. This S-Box swaps all 16 input bytes. Then, the result comes out arranged in four rows and four columns.[5]

2. Shift Rows:

In the matrix, every row moves to the left. If any elements fall off the left side, they pop back in on the right side. This shifting happens like this:

The first row remains unchanged.

The second row shifts one step to the left. The third row shifts two steps to the left. The fourth row shifts three steps to the left.

The resultant matrix will consist of the same 16 bytes but shifts with respect to each other.

3. MixColoumns:

The MixColoumns step is one of the four main steps performed on the state matrix. It works during each round of encryption. The purpose of MixColoumn step is to yield diffusion by mixing the columns of the state

matrix which then helps in the spreading of influence of each byte in the entire block. It helps in increasing the complexity of the cipher and it makes cipher more resistant to cryptic attacks.[5]

4. Addroundkey:
The Addroundkey step is super important in both encrypting and decrypting. It's where it mixes up the data being processed with a special key made from the original encryption key, using a special math operation called XOR. The matrix which is of 16 bits are considered as 128bits and then the 128 bits of the round key are combined using the XOR operation.[5]

5. Decryption Process:
Decrypting in AES is like going backward through the steps used for encrypting. AES decryption consists of performing the inverse of each step that has been performed during encryption.

Each round goes through four steps, but in reverse:
- Add the round key.
- Mix the columns.
- Shift the rows.
- Substitute the bytes.

The implementation of encryption and decryption algorithms takes place separately, but they are related to each other.

V. METHODOLOGIES

1. Secure Login:
The user must login into the account through the portal. If the login credentials provided by the end user are incorrect then the end user will not be able to access login. The encryption is accessed directly when the user enters the login details and uploads the file on cloud system.

2. Encryption:
The file will be encrypted using AES technique and then will be uploaded to the cloud. It's symmetric, which means the user uses the exact same key for both encrypting and decrypting. AES operated on fixed size blocks of data. It is used in different applications and is highly secure. While encrypting the server will add a few sets of words/symbols at the end of the text file.

3. Uploading Encrypted File:
The file will be encrypted using AES technique and then will be uploaded to the cloud. If any individual bypasses the security of cloud storage, then he would get the access of encrypted file only. Thus, ensuring dual security. First, provided by the AWS cloud and second by AES encryption technique. Thus, ensuring the confidentiality of the file is maintained.

4. File Decrypt:
When a user wants to access the file of the owner, the user is asked for a secret key (which was used to encrypt the file). On entering the secret key, the text would be decrypted using that key. If the last set of words is equal that of original padded sentences by the encryptor.

5. Downloading Decrypted File:
The file is decrypted and downloaded. However, if the user does not enter the accurate key then the file will not decrypt and shows the warning.

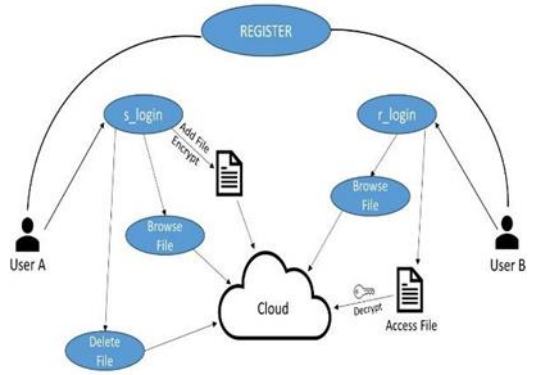

Figure 4: Architecture of secure file sharing system.

Figure 4 explains how the users will interact with the server and the S3 cloud bucket.

Users will use the UI (web application) to register on the server. After the successful registration, A user named ‘User-A’ can upload a file, which will be encrypted using the AES encryption algorithm; following that, it will be stored in the S3 bucket. Users can also perform other functions like ‘browse files’ and ‘Delete files. On the other hand, if another user, ‘User-B’, wants to access a file from a remote location, he can browse the files and request access for the particular file. User-B will then receive a key, which

the user will use to decrypt the file and read its contents.

CONCLUSION

In this paper, the main aim of the system is to access data and store it. Data sharing is done securely in a cloud environment. The sharing can only be controlled by the owner of data. Many techniques are used to provide security to file. In this paper we used AES to enhance the security of shared files. As storage we the AWS cloud is used which used S3 bucket which already had provided the first level of security. With the help of security mechanisms, we achieved better data integrity, and better data confidentiality.

REFERENCES

[1] Joseph Selvanayagam, Akash Singh, Joans Michael, Jaya Jeswani, "Secure File Storage on Cloud Using Cryptography",2018.

[2] S. A. Jadhav, A. S. Abhang, R. A. Patil, pune vidyarthi griha's coe, maharashtra, and india, "SECURE FILE STORAGE AND SHARING ON CLOUD USING AES ALGORITHM", IJARIIE, vol. Vol-4, no. Issue-3, pp. 1663–1665, 2018.

[3] R. B. Madhumala, S. Chhetri, A. Kc, and H. Jain, "Secure File Storage & Sharing on Cloud Using Cryptography", International Journal of Computer Science and Mobile Computing, vol. 10, no. 5, pp. 49–59, May 2021, doi: 10.47760/ijcsmc.2021.

[4] GfG, "Advanced Encryption Standard (AES)," GeeksforGeeks, May 22, 2023. https://www.geeksforgeeks.org/advanced-encryption-standard- aes/

[5] S. Malviya and S. Dave, "Secure Data Sharing Scheme using Cryptographic Algorithm for Cloud Storage", Research India Publications, journal-article, 2018.

[6] Abhishek Saini, Chaman Sharma, Nadeem Khan, "Paper on AWS",2024.

[7] https://aws.amazon.com/what-is-aws/

[8] https://www.techtarget.com/searchstorage/definition/cloud- storage

[9] Uttam Kumar, Mr. Jay Prakash, "Secure File Storage on Cloud Using Hybrid Cryptography Algorithm",2020.

[10] G. Verma and S. Kanrar, "A novel model to enhance the data security in cloud environment", ResearchGate, Apr. 2015.

[11] Ashalatha R, "A survey on security as a challenge in cloud", 2012.

[12] M. Sharma, A. Sharma, "A secret file sharing scheme with chaos-based encryption", 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Kanpur, India, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944344.

[13] https://en.wikipedia.org/wiki/Cloudcomputingarchitecture

[14] A. Kumar, B. G., Lee, H. Lee, & A. Kumari,"Secure storage and access of data in cloud computing",2012 International Conference on ICT Convergence (ICTC), Jeju, Korea (South), 2012, pp. 336-339, doi: 10.1109/ICTC.2012.6386854.