IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304416 |

Encryption and Decryption of Files using AES Algorithm on Cloud Platform

Akshath Anchan, Aayush Gade, Shravani Gaikwad, Tannu Singh, Prof. Nirmol Munvar

U.G. Student, Department of Electronics and Computer Science, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

U.G. Student, Department of Electronics and Computer Science, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

U.G. Student, Department of Electronics and Computer Science, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

U.G. Student, Department of Electronics and Computer Science, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

Assistant Professor, Department of Electronics and Computer Science, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

ABSTRACT: This paper discusses the significance of encryption and decryption of files which are on cloud platforms. Nowadays due to advancement in cloud computing information is being stored more on cloud Platform and dropbox and google drives provide cloud services to users with low cost storage. It emphasizes enhancing data security through advanced cryptographic techniques. The aim is to implement AES encryption and decryption methods to safeguard files and ensure confidentiality and integrity of sensitive information. The application of AES algorithm for file protection, emphasizing the importance of encryption in mitigating cyber threats and unauthorized access to cloud-stored data.

KEYWORDS: Encryption, Decryption, Cloud computing, Advanced Encryption Standard, Dropbox.

I. INTRODUCTION

The advnacement in cloud computing has led to a significant shift in how individuals and organizations store and access their data. Services like Dropbox and Google Drive offer users low-cost cloud storage solutions, allowing them to conveniently store and share files remotely.Although, the increasing reliance on cloud platforms raises concerns about the security and privacy of sensitive data.

So, encryption of files containing sensitive data is one method to achieve enhanced security by the use of the Advanced Encryption Standard (AES), a widely recognized symmetric encryption algorithm. AES gives a robust and efficient method for encrypting and decrypting data, ensuring the confidentiality and integrity of cloud-stored files.

This paper aims to implement AES encryption and decryption for files stored on cloud platforms. The research emphasizes on the strengths of AES to safeguard sensitive information, mitigating the risks associated with unauthorized access or data breaches in cloud environments. The paper aims to contribute to the ongoing efforts in enhancing the security and privacy of cloud-based data storage and sharing.

In this paper implementation of 128 bit Advanced Encryption Standard (AES) technique is done for encrypting and decrypting the content of files stored on cloud platforms. AES-128 is considered secure against brute-force attacks, as it would take an extremely long time to try all possible 128-bit keys.3 However, side-channel attacks and implementation vulnerabilities can still pose risks.[1][6][3]

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304416 |

II. LITERATURE SURVEY

A. Advance Encryption Standard (AES) algorithm

AES is a widely adopted symmetric encryption algorithm that provides robust data protection.AES is widely used for encrypting data stored in cloud environments, providing a robust barrier against unauthorized access.[2]

Client-side encryption using AES can add an extra layer of security, even if the cloud storage system is compromised.AES-based encryption is crucial for ensuring the confidentiality and integrity of sensitive data stored in the cloud.[2][4]

AES operates on 128-bit blocks of data and supports key sizes of 128, 192, and 256 bits.The AES algorithm performs multiple rounds of operations, including SubBytes, ShiftRows, MixColumns, and AddRoundKey, to encrypt and decrypt data.In this paper 128 bit advance encryption standard algorithm i.e (AES -128) . The AES-128 algorithm is considered secure against brute-force attacks due to the large key space. Many modern CPUs have built-in hardware instructions for AES-128, which can improve the speed and security of the encryption process.Hardware acceleration of AES can help protect against timing-related side-channel attacks.[3]

B. Encryption Process of (AES -128) Advance Encryption Standard algorithm

1. Key Expansion:

- The 128-bit AES encryption key is expanded into 11 round keys (1 initial key and 10 round keys).
- This key expansion process generates the necessary keys for each round of the encryption algorithm.

2. Initial Round :

- The 128-bit plaintext block is arranged in a 4x4 state array.

The state array is XORed with the initial round key (K0) in the "Add Round Key" step

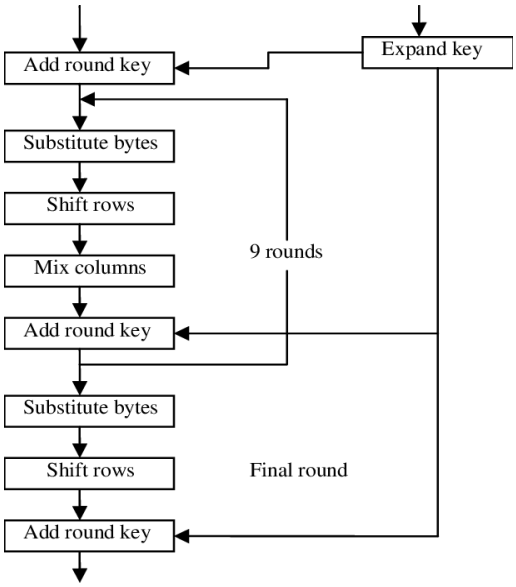

fig 1. Encryption using AES -128 algorithm

3. Round 1-9 :

- The state array undergoes the following steps in each of the 9 rounds:
- SubBytes: Each byte in the state array is substituted with a value from a predefined S-box.
- ShiftRows: The rows of the state array are shifted cyclically by different offsets.
- MixColumns: The columns of the state array are combined using a linear mixing operation.
- Add Round Key: The state array is XORed with the corresponding round key.

4. Final Round :

- The final round skips the MixColumns step and only performs:

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304416 |

- Sub Bytes.
- Shift Rows.
- Add Round Key (with the final round key)
- The resulting state array is the final 128-bit ciphertext

C . Decryption Process of (AES -128) Advance

ENCRYPTION STANDARD ALGORITHM

1. Key Expansion:
- The 128-bit AES decryption key is expanded into 11 round keys (1 initial key and 10 round keys).
- This key expansion process generates the necessary keys for each round of the decryption algorithm.

2. Final Round :
- The 128-bit ciphertext block is arranged in a 4x4 state array.
- The state array undergoes the following steps in the final round:
- Inverse Shift Rows: The rows of the state array are shifted cyclically in the opposite direction compared to the encryption process.
- Inverse Sub Bytes: Each byte in the state array is substituted with a value from the inverse S-box.
- Add Round Key: The state array is XORed with the final round key.

3. Round 1-9 :
- The state array undergoes the following steps in each of the 9 rounds:
- Add Round Key: The state array is XORed with the corresponding round key.
- InvMixColumns: The columns of the state array are combined using the inverse linear mixing operation.
- InvShiftRows: The rows of the state array are shifted cyclically in the opposite direction compared to the encryption process.
- InvSubBytes: Each byte in the state array is substituted with a value from the inverse S-box.

4. Initial Round :
- The state array is XORed with the initial round key (K0) in the "Add Round Key" step.
- The resulting state array after the decryption process is the original 128-bit plaintext block.

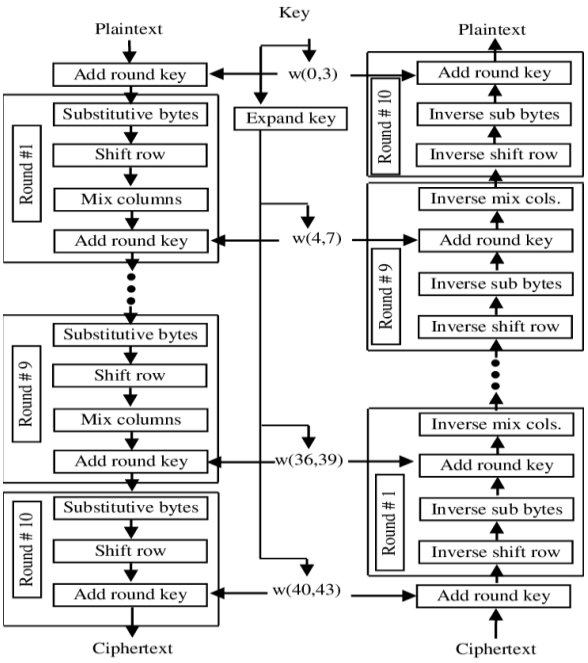

Fig.2 Decryption using AES -128 algorithm

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304416 |

III. SYSTEM DESIGN

We proposed a method which enhances the security of cloud platform services like dropbox. This system provides access to the users according to their roles and responsibilities and permissions related to a particular role is predefined. This access will be associated with the email id and password given by the administrator or higher authority although password can be changed as per requirement.

So, now users need to login with the given email id and password to get the access of the system to upload, delete , access , download the file from the dashboard. Here the dashboard is developed on a cloud platform.[6]

When a user uploads any file on the dashboard, the system will start reading the content of the file and initiate the process of encryption using the AES-128 algorithm . When a user wants to access or download any file from the dashboard then the system will first initiate the decryption process using AES-128 algorithm. After the completion of the decryption process the content of the file will be directed to a browser so that the user can access the file and download the file.[2][4][7]

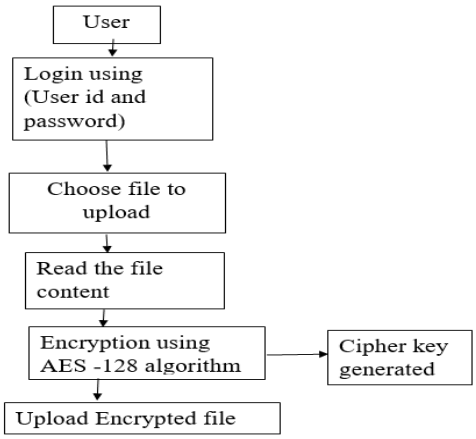

Fig.3 Encryption process

Decryption process of encrypted file is demonstrated in below diagram :

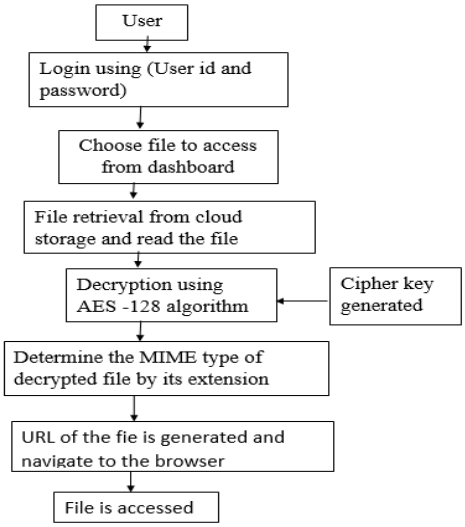

Fig.4 Decryption process

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304416 |

IV. IMPLEMENTATION

AWS is streamlined through integration with GitHub and AWS Amplify hosting. After configuring the deployment environment and performing necessary setup tasks, the project is provisioned, built, and deployed. Enhancements to the project include user interface improvements, authentication refinements, encryption enhancements, audio-video support, resolution of navigation and button functionality issues, deployment optimization, and multi-purpose system adaptation.[1][6]

To upload a file to AWS, bucketname is needed where we want to upload the file. A key (filename) is needed under which the file will be stored in the bucket. A params object is created which will have bucketname and filename. Then the s3.upload() method provided by the AWS SDK for JavaScript is used to initiate the upload operation. This method takes the params object as its first parameter and a callback function as its second parameter. Inside the callback function it checks for errors. If an error occurs, an error message is logged.[8]

To delete a file from AWS bucketname is needed from where we need to delete the file. A key (filename) is needed which we want to delete from the bucket. A params object is created which will have bucketname and filename. Then the s3.deleteObject() method provided by the AWS SDK for JavaScript is used to initiate the delete operation. This method takes the params object as its first parameter and a callback function as its second parameter. Inside the callback function it checks for errors. If an error occurs, an error message is logged.[6]

V.RESULTS

In this paper parameters such as Security level, Speed, Data confidentiality, Data integrity and Ciphertext size are analyzed . These parameters are important to compare various algorithms. This performance evaluation analysis helped us to get to know that the AES-128 algorithm will provide security for protection of files stored on cloud platforms.[5] The performance was observed by considering the parameters such as security, speed, Data confidentiality, Data Integrity etc. The results are discussed below.

Parameters	AES	DES	Blowfish
Security	Very Secure	Not Secure	Secure
Speed	Very Fast	Very Slow	Fast
Data Confidentiality	Yes	No	Yes
Data Integrity	Yes	No	Yes
Cipher text	Larger than plain text	Same as plain text	Same as plain text

TABLE I. COMPARISON OF PROPOSED WORK WITH EXISTING METHODS

The content of a file which is encrypted based on 128 bit key (AES-128) encryption is experimented on formats such as pdf files, text files, document files, image files, excel file. All these files are encrypted with AES-128 bit encryption . The result is analyzed with the original files and displayed in the table below. It is observed that the variation between the original file and the encrypted file is not based on size of the file but on the format of the file. [6]

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304416 |

Data Format	Size of original data (in bytes)	Size after 128 bit key encryption (in bytes)
.pdf	23,91,839	23,91,840
.txt	5,882	5,888
.docx	12,448	12,448
.jpg	1,07,748	1,07,760
.xls	1,83,296	1,83,312

TABLE II. THE COMPARISON OF SIZES WITH ORIGINAL DATA AND ENCRYPTED DATA

VI. CONCLUSION

This paper has presented a comprehensive study on the implementation of AES encryption and decryption for files stored on cloud platforms. The proposed framework leverages the strengths of the AES algorithm to provide robust data protection, ensuring the confidentiality and integrity of sensitive information in cloud environments.
The implementation of client-side encryption, in addition to server-side encryption, adds an extra layer of security, even if the cloud storage system is compromised.Future work may explore the integration of the AES encryption framework with emerging technologies, such as blockchain and attribute-based access control, to further strengthen the security and access management of cloud-stored files.

REFERENCES

[1]"Cloud Computing Security: Amazon Web Service," *IEEE Conference Publication | IEEE Xplore*, Feb. 01, 2015. https://ieeexplore.ieee.org/document/7079135
[2]"Framework for client side AES encryption technique in cloud computing," *IEEE Conference Publication | IEEE Xplore*, Jun. 01, 2015. https://ieeexplore.ieee.org/document/7154763
[3]"Secure File Storage on Cloud using Hybrid Cryptography," *IEEE Conference Publication | IEEE Xplore*, Oct. 22, 2021. https://ieeexplore.ieee.org/document/9702323
[4]"An implementation of AES-128 and AES-512 on Apple mobile processor," *IEEE Conference Publication | IEEE Xplore*, Jun. 01, 2017. https://ieeexplore.ieee.org/document/8096255/
[5] "Advanced Encryption Standard Algorithm with Optimal S-box and Automated Key Generation," *IEEE Conference Publication | IEEE Xplore*, Apr. 28, 2022. https://ieeexplore.ieee.org/document/9823662/
[6]"Access control for the cloud based on multi-device authentication," *IEEE Conference Publication | IEEE Xplore*, Aug. 01, 2015. https://ieeexplore.ieee.org/document/7345365
[7] "Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud," IEEE Conference Publication | IEEE Xplore, Sep. 01, 2015. https://ieeexplore.ieee.org/document/7375144
[8]"Efficient and secure file transfer in cloud through double encryption using AES and RSA algorithm," IEEE Conference Publication | IEEE Xplore, Mar. 05, 2021. https://ieeexplore.ieee.org/document/9397005

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details