© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 03 | April - June 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

Special Edition
NCASIT 2023, 29th April 2023
Department of Computer Engineering,
St. Vincent Pallotti College of Engineering & Technology, Nagpur,

SECURED FILE STORAGE ON THE CLOUD USING AES-CBC ENCRYPTION

Ashwin Paul
Computer Engineering
St. Vincent Pallotti College of
Engineering & Technology
Nagpur, India.

Jatin Lakhorkar
Computer Engineering
St. Vincent Pallotti College of
Engineering & Technology
Nagpur, India.

Komal Jaisinghani
Assistant Professor

Computer Engineering Department
St. Vincent Pallotti College of
Engineering & Technology
Nagpur, India.
Computer Engineering
St. Vincent Pallotti College of
Engineering & Technology
Nagpur, India.

Nupoor Chorwahe
Computer Engineering
St. Vincent Pallotti College of
Engineering & Technology
Nagpur, India.

Abstract---Cloud computing is a model that treats internet resources as a unified entity or cloud. One essential issue in cloud computing is data security, which is handled using cryptography methods. A possible method to encrypt data is Advanced Encryption Standard (AES). This paper proposes a method for providing different security services like authentication, authorization, and confidentiality. AES-CBC 256-bit symmetric encryption is used to increase data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded to a cloud. The encryption key is derived from the password and a random salt using PBKDF2 derivation with 10000 iterations of SHA256 hashing.

Keywords---cloud computing and storage, encryption-decryption

I. Introduction

The term "cloud" describes the practice of keeping user data off of their own computer's hard drive and instead storing it in a remote database. The cloud eliminates the requirement for building up a company's own data center or server by providing computing resources as a service in a scalable manner to the clients via the Internet. Customers pay according to their amount of utilization and these resources are available on demand. Storage, processing power, applications, and services are all part of the resource pool. Cloud
Dipali Kambale computing has resulted in numerous innovative computing reforms. Cloud computing is an internet-based technology that delivers services via the internet. When it comes to service quality, data security is crucial. Cloud computing constantly presents fresh security issues for a variety of reasons.

Due to its many benefits, such as on-demand network access with low costs based on user consumption, cloud computing is a popular model for distributed data storage. But, because the cloud service provider has access to all of the data, it presents numerous security issues. There have been numerous proposals for maintaining security and privacy in the cloud, including encryption, replication, VM isolation, etc. [3], but the majority of these have focused on single cloud environments, where all data is stored on a single public cloud, raising security concerns because a malicious administrator has full access to the data and could use it for evil purposes. The vendor-lock-in problem results in the loss of all information in the event that the service provider suspends his operations and the loss of data integrity as a result of unlawful data change.

Our goal is to develop a system that secures user data. The initial step in using cloud services is registering as a user. Everywhere in the built-in network the user can access files. After properly registering, a user cannot access services until the administrator approves their request. The administrator manages the user's registration by approving or refusing the user's request. The user can now carry out the different file operations after receiving authorization. These file operations include uploading, downloading, deleting, updating, and other activities on files. Each user is given a set amount of memory to use for their own file operations. One of the most crucial aspects that consistently annoys the user is security. To secure user logins, we'll employ encryption and decoding techniques. The encryption algorithms are AES-CBC 256-bit symmetric encryption. The encryption key is derived from the password and a random salt using PBKDF2 derivation with 10000 iterations of SHA256 hashing.

II. Objective

The main objectives of the system are:

1) To securely store and retrieve data on the cloud that is only controlled by the owner of the data.
2) To provide strong access controls and data encryption to prevent unauthorized entities from accessing confidential information.
3) To secure the user's data using various cryptographic algorithms.

III. Literature Review

This project implements a double-stage encryption algorithm that provides high security, scalability, confidentiality, and easy accessibility of multimedia content in the cloud. The system uses two different hybrid approaches for encryption and decryption, namely AES and RSA algorithms, and AES and Blowfish algorithms, and shows a comparative study on the difference between the two approaches [1]. The main goal is to securely store and access data in the cloud that is not controlled by the owner of the data. In this paper an approach is used that ensures the security and privacy of client-sensitive information by storing data across a single cloud, using AES, DES, and RC2 algorithms [2].

This paper facilitates the use of encoding the encrypted files and sharing files in the encrypted format itself. This paper uses the techniques of both encrypting and sharing the data. Erasure encoding supports sharing of encrypted files and is valid in decentralized distributed systems. A distributed erasure code is used to authorize data safety in dispersed cloud storage [3]. This paper deals with various issues associated with security and focuses mainly on data security and methods of providing security by data encryption. Various encryption methods of block cipher algorithms such as Triple DES and Blowfish are discussed for providing solutions to the cloud [4]. A comprehensive analysis explored the foremost techniques concerning the functionality and the relevant solutions to share the data securely for data protection in the cloud environment. The essential and adequate information which is desired to fetch the core of the method along with the research gaps and future directions about each discussed solution is highlighted. Furthermore, exhaustive analysis and a comparison among the refereed techniques are performed. The relevancy of every technique is analyzed in compliance with the context [5].

In this paper, an improved security in cloud storage framework using different encryption algorithms like AES algorithm with S- box and Feistel Algorithm. The structure utilizes the information-transferring, cutting, ordering, encryption, merging, unscrambling and recovery cycle to make sure about the enormous information put away in the multi-cloud. With the help of AES, and Feistel algorithm achieved high performance as compared to other algorithms [6]. In this paper, a multi-security-level cloud storage system that is combined with AES symmetric encryption and an improved identity-based proxy re-encryption (PRE) algorithm scheme is implemented. It integrates fine-grained delegation based on the element of type and heterogeneous features that can transform ciphertext from IBE-type to PKE-type text. The fine-grained features mean that the data owner can share private data using a fine-grained approach, e.g., adding a single file or a class of files. The feature of heterogeneity greatly improves the performance of the algorithm and at the same time makes it more convenient and compatible with the system developed based on the traditional PKE encryption algorithm [7]. In this paper, they mitigate the vulnerability of possible attacks by Yu et al. ID-based remote data integrity checking protocol by formalizing a more secure model using AAA services. They provided a novel model for untrusted PKG. Our scheme is more secure, highly efficient, and practical. The experimental evaluations show that this scheme is more efficient than known ones [8].

This paper introduced a new approach for protecting data privacy from attackers who retroactively obtain, through legal or other means, a user's stored data and private decryption keys. A novel aspect of the SeDas approach is the leveraging of the essential properties of the active storage framework based on the T10OSD standard. SeDas: self-destructing data system based on the active storage framework of cloud computing gives the most optimum solution to protect the important and private data of the user from any kind of attack. SeDas causes sensitive information, such as account numbers, passwords, and notes to irreversibly self-destruct, without any action on the user’s part. This SeDas system will help to provide researchers with further valuable experience to inform future object-based storage system designs for cloud services [9]. In this paper, the proposed system will help the user/people to store their files, and documents on the local cloud and can also perform various operations on the files such as file upload, delete, append, zip file, etc. Also, security is provided at the login point by applying an encryption-decryption technique. The Two-way handshake protocol is also used for user authentication. By using this Two-way handshake-protocol it assures the user that except the user no one can log in with the user’s Id and view the stored files and documents [10].

This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid encryption is used where files are encrypted by blowfish coupled with file splitting and SRNN (modified RSA) is used for the secured communication between users and the servers.[11]

IV. Cloud storage using AES.

AES Algorithm

A symmetric block cipher algorithm with a block size of 128 bits is the AES Encryption algorithm, also referred to as the Rijndael algorithm. These distinct blocks are converted using keys that are 128, 192, and 256 bits long. It then connects these blocks to create the ciphertext after encrypting each one separately.

It is founded on an SP network, also referred to as a substitution-permutation network. It comprises a number of interconnected processes, some of which involve bit shuffles and others involve substituting inputs with particular outputs (substitutions). (permutations).

A. Byte Substitution (SubBytes)

By accessing a fixed table (S-box) provided in the design, the 16 input bytes are replaced. A matrix with four rows represents the outcome.

B. Shiftrows

Each of the matrix's four rows has a left shift. Any entries that "fall off" are then reinserted on the row's right side. The following is how a shift is conducted:

The top row has not been shifted. The third row is moved to two positions to the left, and the second row is moved to one (byte) position to the left.

There is a three-position leftward movement in the fourth row. The outcome is a new matrix with the same 16 bytes but shifted relative to one another.

C. MixColumns

Now, a unique mathematical function is used to change each column of four bytes. This function accepts the four as arguments. Bytes from a single column and produce four entirely new bytes to replace the first column. The outcome is another new matrix with 16 more bytes. It should be noted that the final round does not include this phase.

D. Addroundkey

The 128 bits of the round key are XORed with the 16 bytes of the matrix, which are now thought of as 128 bits. The output is the ciphertext if this is the final round. If not, the resulting 128 bits are translated into 16 bytes, and the process starts all over again.

D. Decryption Process

An AES ciphertext's decryption procedure is quite identical to its encryption procedure in reverse. every round includes the four steps carried out in reverse order.

- Add round key.
- Mix columns
- Shift rows
- Byte substitution

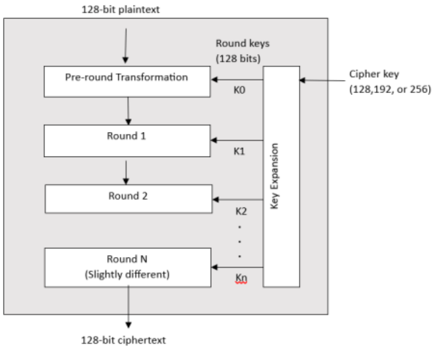


Fig-(1) AES block diagram

CBC (short for cipher-block chaining) is an AES block cipher mode that trumps the ECB mode in hiding away patterns in the plaintext. CBC mode achieves this by XOR-ing the first plaintext block (B_1) with an initialization vector before encrypting it. CBC also involves block chaining as every subsequent plaintext block is XOR-ed with the ciphertext of the previous block. In this version, for Advanced Encryption Standard (AES) processing ability, the cipher key length is 128/192/256 bits for AES. Another limitation is that our working mode works on units of a fixed size (64 or 128 bits for 1 block), but text in the real world has a variety of lengths. So, the last block of the text provided to this primitive must be padded to 128 bits before encryption or decryption.

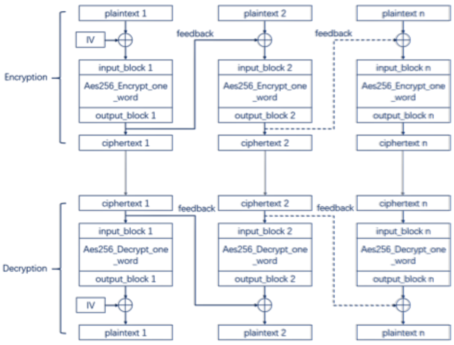
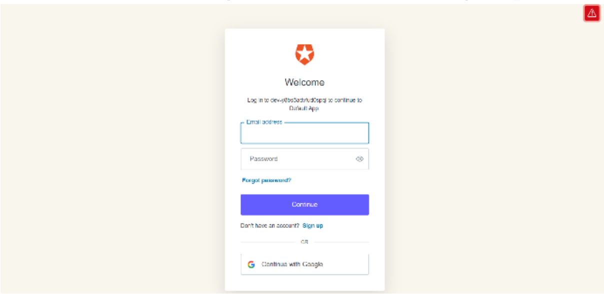


Fig-(2) AES-CBC256 flowchart

In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key. In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size. For example, a 512-bit string of data would be transformed into a 256-bit string through SHA-256 hashing. Three properties make SHA-256 secure. First, it is almost impossible to reconstruct the initial data from the hash value. A brute-force attack would need to make 2^{256} attempts to generate the initial data. Second, having two messages with the same hash value (called a collision) is extremely unlikely. With 2^{256} possible hash values (more than the number of atoms in the known universe), the likelihood of two being the same is infinitesimally, unimaginably small. Finally, a minor change to the original data alters the hash value so much that it's not apparent the new hash value is derived from similar data; this is known as the avalanche effect.

V. Implementation

[1] The user enters the necessary credentials required for signing up and login purposes i.e. g-mail id and password for the user profile or can have direct access using a continue with Google option.



Welcome

Log in to dev-y8bs3advfud0spqj to continue to Default App

Email address

Password

Forgot password?

Continue

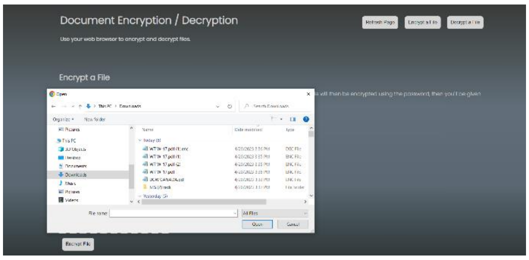
Don't have an account? Sign up

OR

Continue with Google

(i) User credentials and login phase

[2] The user selects the file to be encrypted.



Document Encryption / Decryption

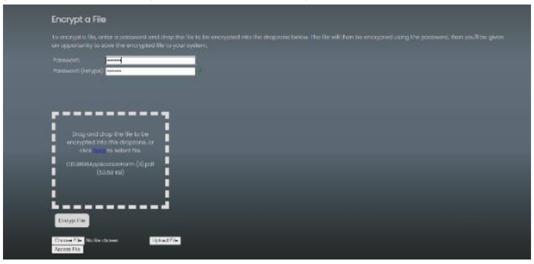
Use your web browser to encrypt and decrypt files.

Encrypt a File

...will then be encrypted using the password, then you'll be given

(ii) file selection phase

[3] File encryption using AES-CBC symmetric encryption with a secret key for access afterward.



Encrypt a File

To encrypt a file, enter a password and drop the file to be encrypted into the dropzone below. The file will then be encrypted using the password, then you'll be given an opportunity to save the encrypted file to your system.

Password ••••••••

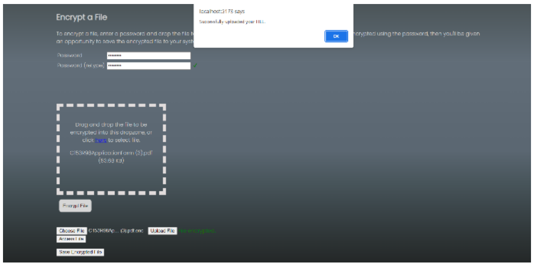
Password (retype) •••••••• ✓

Drag and drop the file to be encrypted into this dropzone, or click here to select file.

C153R98ApplicationForm (3).pdf (53.68 KB)

(iii) encryption key and file encryption phase

[4] The user uploads the encrypted file into the cloud and can access the file using a secret key.



localhost:3175 says

Successfully uploaded your file.

Encrypt a File

To encrypt a file, enter a password and drop the file to be encrypted into the dropzone below. The file will then be encrypted using the password, then you'll be given an opportunity to save the encrypted file to your system.

Password ••••••••

Password (retype) •••••••• ✓

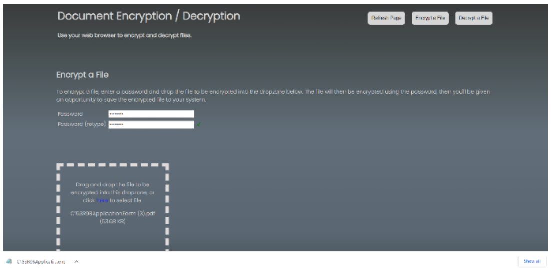
Drag and drop the file to be encrypted into this dropzone, or click here to select file.

C153R98ApplicationForm (3).pdf (53.68 KB)

File encrypted.

(iv) Cloud upload and access phase

[5] The user can download the encrypted file uploaded in the cloud after selecting the necessary file.



Document Encryption / Decryption

Use your web browser to encrypt and decrypt files.

Encrypt a File

To encrypt a file, enter a password and drop the file to be encrypted into the dropzone below. The file will then be encrypted using the password, then you'll be given an opportunity to save the encrypted file to your system.

Password ••••••••

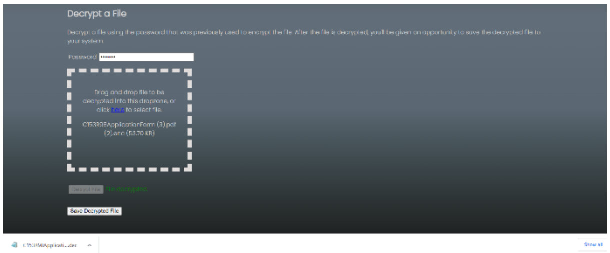
Password (retype) •••••••• ✓

Drag and drop the file to be encrypted into this dropzone, or click here to select file.

C153R98ApplicationForm (3).pdf (53.68 KB)

(v) file download module

[6] The user can download the decrypted file after entering the key credentials created in the early encryption phase.



Decrypt a File

Decrypt a file using the password that was previously used to encrypt the file. After the file is decrypted, you'll be given an opportunity to save the decrypted file to your system.

Password ••••••••

Drag and drop file to be decrypted into this dropzone, or click here to select file.

C153R98ApplicationForm (3).pdf (2).enc (53.70 KB)

File decrypted.

(vi) decryption module

As a result of the system's dual layer of security, the files of the user are secure on the cloud.

VI. Conclusion

In this paper, a functioning cloud storage framework that is secured is taken into consideration. The "AES-CBC" algorithm identifier is used to perform encryption and decryption using AES in Cipher Block Chaining mode. When operating in CBC mode, messages that are not exact multiples of the AES block size (16 bytes) can be padded under a variety of padding schemes. To guarantee the highest level of security, we used the AES-in CBC mode in the suggested system.

VII. Future Scope

As for the future scope of AES CBC encryption, it is expected to continue to be a popular and widely used encryption algorithm for secure communication and data protection. However, there are some concerns about the security of CBC mode, particularly when used with padding schemes that are vulnerable to certain attacks, such as the padding oracle attack. As a result, there has been a shift towards using authenticated encryption modes, such as AES GCM or AES CCM, which provide both confidentiality and authenticity

.

VIII. References

[1] Shruti Kanatt, Amey Jadhav, and Prachi Talwar (2020). Review of Secure File Storage on Cloud using Hybrid Cryptography. International Journal of Engineering Research & Technology (IJERT).

[2] Joseph Selvanayagam1, Akash Singh2, Joans Michael 3, Jaya Jeswani4(2018). SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY. International Research Journal of Engineering and Technology (IRJET)

[3] R.Nivedhaa and J.Jean Justus(2018). A Secure Erasure Cloud Storage system using Advanced Encryption Standard algorithm and Proxy Re-encryption. International Conference on Communication and Signal Processing

[4] Dr.M.Naveetha Krishnan, Mr. T.Tamilarasan (2021) SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY. International Journal of Advanced Research in Computer Science Engineering and Information Technology.

[5] ISHU GUPTA 1, (Member, IEEE), ASHUTOSH KUMAR SINGH 2, (Senior Member, IEEE), CHUNG-NAN LEE1, (Member, IEEE), AND RAJKUMAR BUYYA 3, (Fellow, IEEE) (2022)
Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Direction

[6] Pronika & S.S.Tyagi (2021).
Secure Data Storage in Cloud using Encryption Algorithm Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks

[7] Jinan Shen1,2*, Xuejian Deng1 and Zhenwu Xu1(2019). Multi-security-level cloud storage system based on improved proxy re-encryption.

[8] Abdul Rehman1,2, LIU Jian1,2, Muhammad Qasim Yasin1,3 and LI Keqiu1,2(2021)
Securing Cloud Storage by Remote Data Integrity Check with Secured Key Generation

[9] Ms. Dhanashri R. Kulkarni1, Mr. Hasib M. Shaikh.
Study & Review of Self Destructing Data System: SeDaS for Secure Cloud Storage.International Journal of Engineering Research & Technology (IJERT).

[10] Hemangi Patel *1, Pratiksha Patil*2, Shardul Patil*3 ,Onkar Kawathe*4(2020).
SECURE CLOUD STORAGE SYSTEM. International Research Journal of Modernization in Engineering Technology and Science

[11] Swarna C#1, Marrynal S. Eastaff*2 (2018)
Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm
IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES