RESEARCH ARTICLE OPEN ACCESS

Providing Security by Encryption and Splitting Technique over Cloud Storage

Jolly Dutta [1],Kanika Gupta [2], Abhishek Chaudhary[3], Avinash kumar Sharma [4]

[1,2,3] Student, [4]Assistant professor ,Department of Computer Science and Engineering
ABES institute of technology,Ghaziabad,Uttar Pradesh

Abstract:

Cloud computing is known to be a secured technology. It has various applications. Cloud computing is providing its security services and storage services at a very low cost. Privacy and authentication are required at a high degree. There are various approaches to deal with these security issues. Cloud is secure enough from all external theft. Cloud computing provides three kinds of services: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). For data protection in cloud server, cryptography is one of the important methods. Cryptography provides various types of symmetric and asymmetric algorithms to secure the data. Here we use two mechanisms in this paper- data encryption and file splitting. When a user uploads a file it is encrypted using AES encryption algorithm. Then encrypted file is divided into equal parts according to the number of clouds and stored on the cloud. This proposed system enhances the data security on cloud.

Keywords — **Data security, file splitting, AES encryption, Cloud services.**

I. INTRODUCTION

Cloud computing is the wider concept of infrastructure. An important example for this can be as we can manage and store all smart-phones or tablets apps or related data at one location i.e. cloud. So we do not require any further memory space at another end. This provides us with the feature of securing data if one might lose his phone data. Availability, Confidentiality, and Integrity, these three can be called as security goals of data. In modern days Cryptography can be classified into three groups. They are as follows: -

1) Symmetric-key algorithms
2) Asymmetric-key algorithms
3) Hash functions

Cryptographic splitting is also termed as cryptographic bit splitting or cryptographic data splitting. This technique is used to secure data over a computer network. This technique involves various processes like encrypting the data, splitting encrypted data further into smaller data units, distributing those smaller units to various storage locations, and then further encrypting the data at its new location. Due to this process, the data is protected from security breaches, because if an intruder gets access to any one data unit, the information is useless unless he combines with other decrypted data units from other locations to get the complete data.

ENCRYPTION: - Encryption is a process to make hide information keep it as a secret information. The actual process of cryptography is called as encryption. Converting or transforming the data into some another form so that data appears to be meaningless and should be unrecognizable. In other ways, it can define the process of converting plaintext to ciphertext where plaintext act as the input to the encryption process and ciphertext as the output of the encryption process.

DECRYPTION: - Decryption is the process of converting from cipher text back to plain text. Another definition would be like it is the process of transforming or converting

ciphertext to plaintext where ciphertext acts as an input to the decryption process and plaintext as the output of the encryption process.

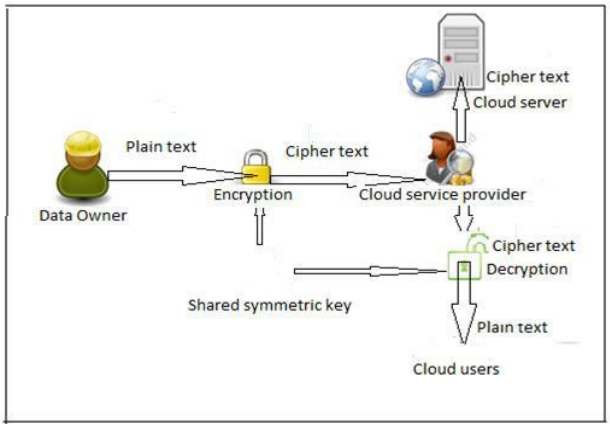


Fig.1 Encryption and Decryption Process

II. BRIEF LITERATURE SURVEY

Vishal R. Pancholi, Dr. Bhadresh P. Patel discussed over the security issues which can be handled by AES encryption algorithm. As the mentioned algorithm the highly secured algorithm for storing data over a cloud and data can be protected against further future attacks called for smash attacks. Their aim is to provide security to data the cloud using AES which has minimal storage space. [1]

Rashmi S. Ghavghave, Deepali M. Khatwar focused on the major issue i.e. data security in cloud computing. This paper proposed the system of Security over multi-cloud. The new architecture has been designed for security of data storage in multicloud using some mechanisms. The architecture developed here is more secure than the existing one as the existing one has the feature of storing the whole file in a single cloud which is not that much secured compare to multicloud. [2]

Anshika Negi, Swati Malik, Dr. Mayank Singh deals with the various security challenges and found a solution
by using security algorithms like split algorithm, DES algorithm, Triple-DES algorithm, AES algorithm. Major portion discussed here is about the process of splitting the file and then encrypting and decrypting it. Further discussion in future will be done by considering security algorithm and by implementing a better vision of split algorithm. [3]

III. MODULES

The following modules are: -

Login and Registration Module: - In registration get a username, email address, password, user generate a random verification code. New Random. Next () is used to generate a random code. The user can sign in and proceed to next step to verification code. Mail is to use email address by using SMTP protocol. The user can verify the code if verification code is blank then redirect to login page else matched then update user status field with text active and redirect the user to the homepage.

FTP Setting Module: - Proposed the system, file get distributed at three different locations. The First location that is our application and next two more FTP where the 2nd and 3rd file is a store. The proposed system, we are designing setting page where this can be further used by an application to upload and download a file from a created table. Insert into table FTP details.

Upload and Download module
Develop a web interface to upload and download files in cloud storage. The different file uploading links are open. The user can choose the link which we want to upload to a cloud. The User can upload the file to the cloud such as doc file, video, mp3, etc.
The Homepage will show the list of the file uploaded by the user from the user-specific directory. The proposed system, we use data list to show file list. File class to get folder and file details like file name, file size. Upload file by using file uploader control we can let the user select file to be upload.

File encryption technique module

Each cloud has its own server. Developing encryption technique like RSA, AES, DES for file decryption before storing it on a cloud is necessary. In the proposed system, the combination of AES algorithm and SHA-1 algorithm are used for encryption and splitting of a file into multiple portions.

File splitting and clubbing module
In the Proposed system, we are splitting the file into different data units then encode and store it on a different cloud. Metadata necessary for decrypting and moving a file will be stored in metadata management server. The File can club with another file.

IV. AES ALGORITHM

In December 2001, a symmetric-key block named as Advanced Encryption Standard (AES) was published by National Institute of Standards and Technology (NIST). It uses 128 -bit block size with the key size of 128, 192 or 256 bits. As we are using AES-256 in this project. Each full round consists of 4 separate functions named as byte substitution, permutation, arithmetic operation over a finite field and XOR with a key. AES has been adopted by the U.S. government and is now used worldwide. The same key is used here for encrypting and decrypting data. This is known as a secret key. By using the same key, messages are encrypted by the sender and decrypted by the receiver.

Asymmetric algorithms use different keys. One key which is known as public key is used for encryption and other keys which is known as private key used for decryption. Nowadays, no attack against AES exists. Therefore, AES is considered as one of the most preferred encryption standard high- security systems around the world. A Public key is known to the public and the private key is known to the user. AES is most frequently used encryption algorithm. today this algorithm is based on several substitutions, permutations and linear transformations. The Hash functions use a mathematical transformation to irreversibly "encrypt" information. It contains algorithms like Message Digest, Secure Hash Algorithm.

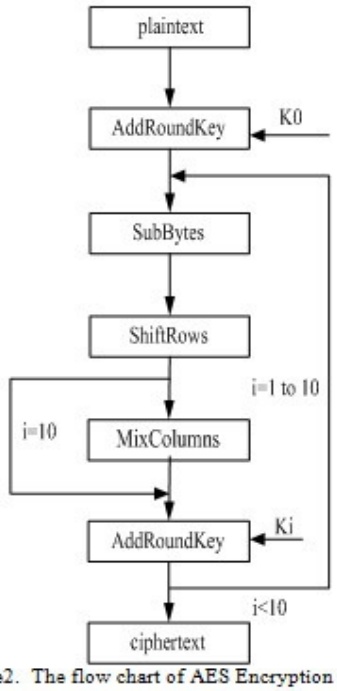


Figure2. The flow chart of AES Encryption algorithm

ALGORITHM:-

A. **The First Step**
- AddRoundKey

The Following Four Functions Are Periodically Repeated

B.
- SubByte
- ShiftRow
- MixColumn
- AddRoundKey

C. **Final Step**
- SubByte
- ShiftRow
- AddRoundKey

D. Byte Substitution (SubBytes):-The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

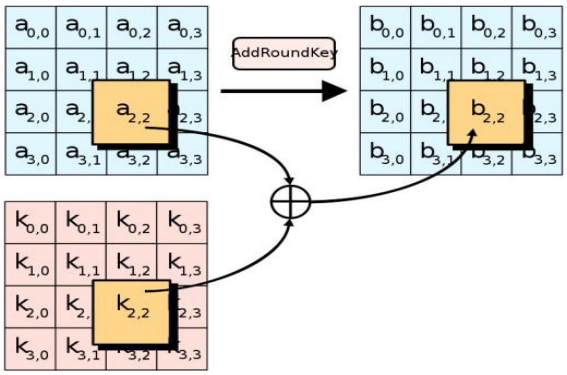


Fig . 2: Byte Substitution (SubBytes)

E. Shift Rows

Each of the four rows of thematrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows

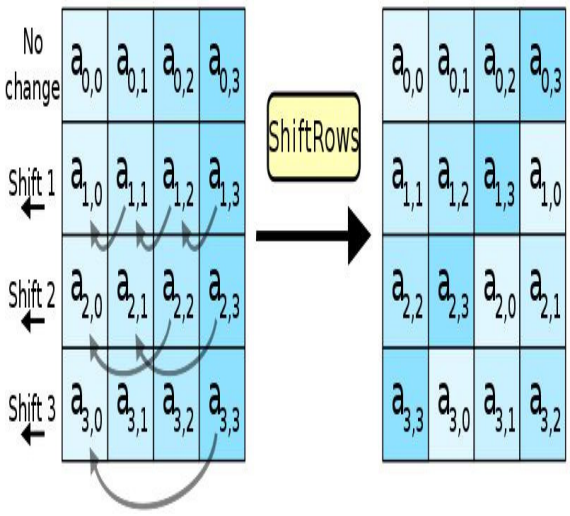
- First row is not shifted.

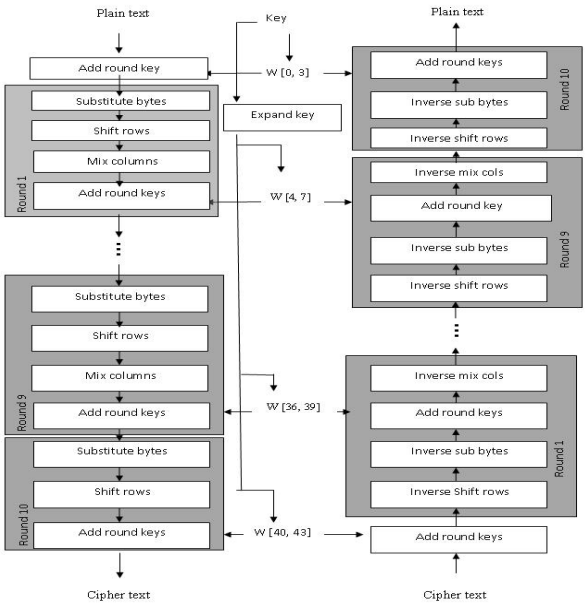
–Second row is shifted one (byte) position to the left.

–Third row is shifted two positions to the left.

–Fourth row is shifted three positions to the left.

–The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.





F. Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

G. Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar rou

V. SPLIT ALGORITHM

In File splitting and clubbing algorithm, we will be splitting the file into different portions then encryption of those split units are to be done and then store it on different cloud server by sharing over the cloud to another user. File clubbing or merging can be done with another file portion. The password is used here by an algorithm to encrypt the different file portions with a unique

number that creates an encrypted file. Now the same password is used to decrypt the file so as to enable the feature of maximum security

Algorithm: -

The encryption is done through the following steps

Step 1: Start the process

Step 2: file name and password is accepted

Step 3: The random number which is generated from the password is unique, as that will serves as a key

Step 4: File and key are split into n parts.

Step 5: The First split of the key is used to encrypt the first split of the file, the second split of the key to encrypt the second split of the file and so on.

Step 6: All splits are Combine to get the file

Step 7: Process is stop

VI. CONCLUSIONS

In this paper, we propose a secure data storage strategy which is capable of addressing the problems of traditional data protection, its methods and improving their security issue and reliability in cloud computing. The two mechanisms that are being followed here are -split algorithm and AES algorithm to provide data security in cloud storage. The function of preventing data from being hacked is done by the split algorithm into different data units. Necessary security is provided by AES before uploading the data.

VII. FUTURE SCOPE

As mentioned there are several security algorithms presently employed in a cloud computing setting. There too several areas that need any enhancements like a lot of economical algorithms may be developed which may increase the safety level within the setting. In future, we would be working on the implementation of the advanced split formula during cloud setting

VIII. REFERENCES

[1] Rashmi S. Ghavghave, Deepali M. Khatwar " Architecture for Data Security In Multi-cloud Using AES-256 encryption algorithm in international Journal on recent And Innovation in Computing International Journal on Recent and Innovation Trends in Computing and Communication. Volume: 3 Issue: 5

[2] Vishal R. Pancholi, Dr. Bhadresh P. Patel "Enhancement of Cloud Computing Security with Secure Data Storage Using AES" in International Journal for Innovative Results in Science and Technology |Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010

[3] Anshika Negi, Swati Malik and Mayank Singh" Data Security in the Cloud" in International Journal of Advanced Research in Computer Science and Software Engineering.