SECURING FILE STORAGE IN CLOUD USING HYBRID CRYPTOGRAPHY

Apurva Garad, Ritika Agrawal, Abhilesh Suryawanshi, Jagadesh Rodagi

SKN Sinhgad Institutes of technology and science
Lonavla, India

ABSTRACT

These days Cloud Computing is used in many different areas like industry, military purposes, colleges etc. to store large amounts of data. The amount of data needing storage is increasing every day and thus, there is a requirement for increased storage space. Retrieval of data at the request of a user on the cloud is easier. Data storing on the cloud comes with some issues. Provide the solution to these issues there is n number of ways. Cryptography techniques are more popular nowadays for data security. The Cryptography technique translates original data into an unreadable form known as ciphertext. Keys are used to converting text or data into unreadable form. Here we have introduced a new security mechanism using an asymmetric key cryptography algorithm. In this proposed system AES-GCM, Fernet, AES-CCM, and CHACHA20_POLY1305 algorithms are used to provide block-wise security to data. The algorithm key size is 128bit, the technique is mainly for key information security. File is split into N parts. Each and every part of file is encrypted using a different algorithm. Encryption of all files takes place simultaneously using different algorithms. Reverse process of encryption is takes place for file decryption purposes.

Keywords—Cloud, Encryption, Decryption, Fernet, Security.

INTRODUCTION

Data is considered the most important thing these days. Cloud storage is a way that allows you to store your data on hosted server. When different organizations use the cloud to store their data, the chances of data misuse increases. To avoid this kind of situations there is an imminent need to secure the data. Also, the data needs to be protected from unauthorized access. This Security concern of protecting the data from unauthorized access can be solved using various ways, the most commonly used techniques are cryptography. The software product is liable to meet the required security needs of data center of cloud. AES-GCM used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The thought of splitting and merging files to achieve the principle of data security. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only an authorized person can access data from the cloud server. Ciphertext data is visible to all people.

OBJECTIVE

The proposed paper is fulfilling the basic security needs and implements data storage using hybrid cryptography. The system for encryption and decryption must be both strong and within the scope of implementation. For this, Hybrid cryptography is implemented. This paper is using some symmetric key cryptography which ensures that the data is secure and also controls authorized access to the data. The Cryptography technique converts the data provided into Cipher text so that no intrusion takes place. The splitting and merging of files achieve the goal of data security.

PROPOSED METHODOLOGY

Encryption of the file:
Step 1: Loading the file on the server.

Step 2: Divide the given file into N parts.

Step 3: Select any of the algorithms and use it for encryption of file.

Step 4: The user gets the public key for this algorithm and a different algorithm is used for securing the keys of cryptography algorithms.

Decryption of the file:

Step 1: Load the key on the server.

Step 2: Decryption of the keys of the algorithms.

Step 3: Use the same algorithms to Decrypt all the N parts of the file which were used to encrypt them.

Step 4: Combining all the N parts to form the original file and provide it to the user for downloading.

A. AES-GCM Algorithm

The combination of AES Counter Mode encryption with Galois Hash authentication (authenticated-encryption) is AES-GCM algorithm.

GCM is constructed from an approved symmetric key block cipher with a block size of 128 bits, such as the Advanced Encryption Standard (AES) algorithm. Thus, GCM is a mode of operation of the AES algorithm.

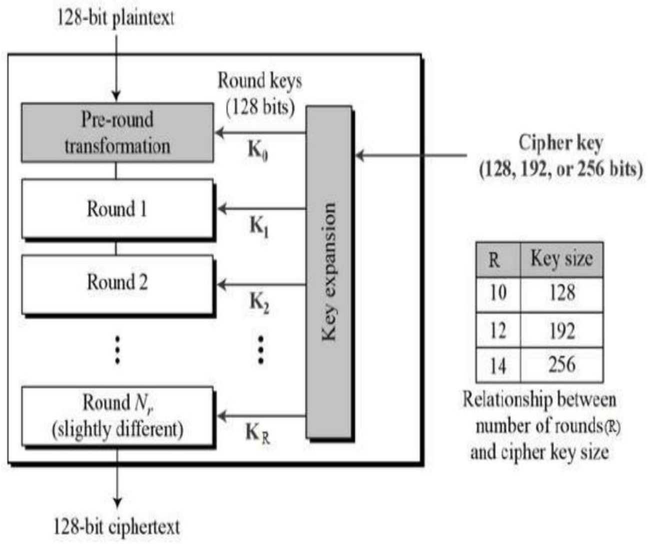

Figure 1: AES-GCM Block diagram

B. CHACHA20_POLY1305

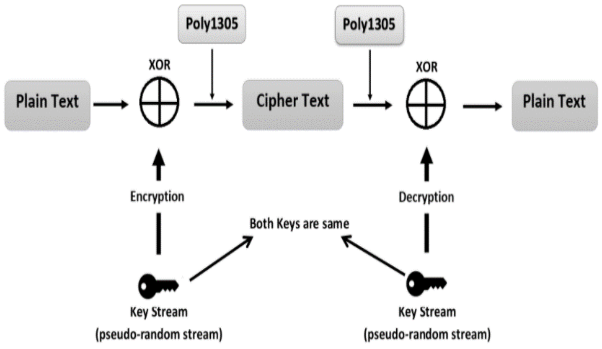

Figure 2: CHACHA20_POLY1305 Block diagram

This algorithm is considered faster than AES is software only implementation which makes it faster on platforms that lack specialized AES hardware. It is a hig speed cipher first described in [Cha-Cha].
This Poly-1305 is a high-level message authentication code which is easy to implement.

C. Fernet Algorithm

Fernet makes sure that a message encrypted applying it cannot be altered or read without the key. It is an implementation of symmetric authenticated cryptography.

Fernet is good for encrypting data that simply fits in memory. It has a design feature that does not expose unauthenticated bytes. It is unsuited for very large files.

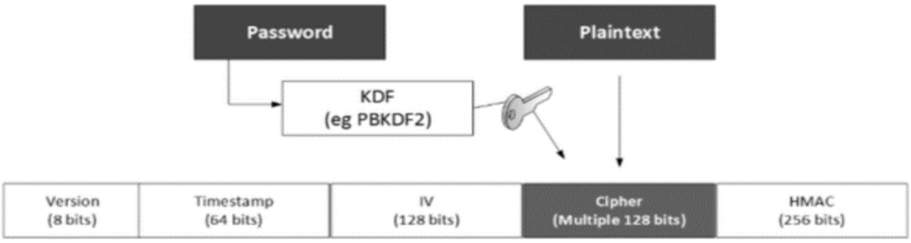

Figure 3: Fernet Block Diagram

D. AES-CCM Algorithm

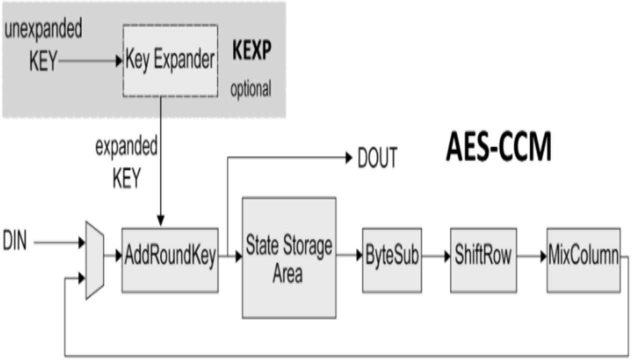

Figure 4: AES-CCM Block diagram

The main role of CCM is to provide authentication and confidentiality during the data transfer. AES-CCM contains inputs that are : an AES key, a nonce, a plaintext, and optional additional authenticated data (AAD). AES-CCM generates two outputs: a cipher text and a message authentication code (also called an authentication tag). CCM is a generic authenticated encryption block cipher mode. CCM is used with the AES block cipher.

PROPOSED WORK

For Encryption
Step 1:
User should fill the registration form.
Step 2:
User will login using their provided credentials.
Step 3:
User requires to upload the file.
Step 4:

Encryption of all the parts of file is done using AES-GCM, FERNET, AES-CCM, CHACHA20_POLY1305.
Step 5:
The file needs to be loaded on AWS Cloud.

For Decryption
Step1:
User should select the file for downloading.
Step2:
User should now provide the credentials (Email ID and name).
Step3:
Email is now sent to the uploader of file
Step4:
If permission is given by file uploader, Load the key on the server.

Step5:
Key is sent to the uploader and downloader of file on their mail ID.
Step6:
Downloader should enter a valid key.
Step7:
Decrypt all the N parts of the file using the same algorithms which were used to encrypt them.
Step8:
Combining all the N parts to form the original file and provide URL link to the user for downloading file.
Step9:
Finally, the file download.

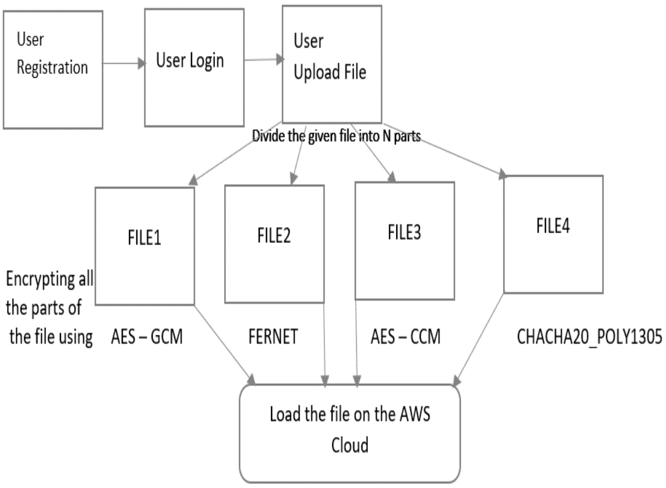
User Registration
User Login
User Upload File
Divide the given file into N parts
FILE1
FILE2
FILE3
FILE4
Encrypting all the parts of the file using
AES – GCM
FERNET
AES – CCM
CHACHA20_POLY1305
Load the file on the AWS Cloud

Figure 1: For Encryption

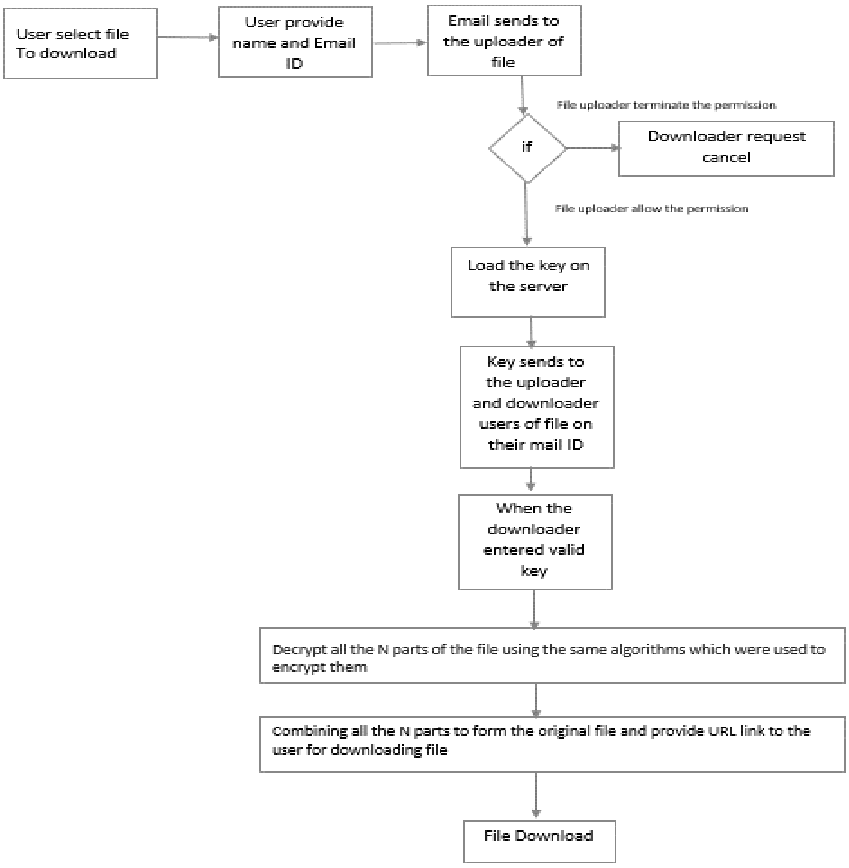
User select file To download
User provide name and Email ID
Email sends to the uploader of file
File uploader terminate the permission
if
Downloader request cancel
File uploader allow the permission
Load the key on the server
Key sends to the uploader and downloader users of file on their mail ID
When the downloader entered valid key
Decrypt all the N parts of the file using the same algorithms which were used to encrypt them
Combining all the N parts to form the original file and provide URL link to the user for downloading file
File Download

Figure 6: For Decryption

CONCLUSION

Cloud can handle the future requirements of accessing multimedia files because of limited capabilities of low configured devices available. But the cloud and its users have many privacy and security related aspects that requires special attention. Data security and privacy protection are the primary problems that need to be solved. The model proposed here is a secure hybrid cryptography approach scenario to provide a safe storage and safe transmission for Confidential Data files. In the future, we can use the proposed model to encrypt and decrypt different files such as different images.

ACKNOWLEDGMENT

I am extremely grateful to, Principal SKN Sinhgad Institute of Technology and Head of Department, Department of Computer Science for providing all the required resources for the successful completion of my project. My heartful gratitude to my project guide Mrs. **Kishori Shimple** Department of Computer Science for valuable suggestions and guidance in the preparation of the report. I express my thanks to the authors of the references and other works of literature referred to in the project.

REFERENCES

[1] Instructions. IEEE Transactions on Computers, 60(1), 135–138. doi:10.1109/tc.2010.147. [2]. Sinaga, M. D., Sembiring, N. S. B., Tambunan, F., & Sianturi, C. J. M. (2018). Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method For Data Security. 2018 6th International Conference on Cyber and IT Service Management (CITSM). doi:10.1109/citsm.2018.8674346.

[2] K. Jasleen and S. Garg, "Security in Cloud Computing using Hybrid of Algorithms", *IJERJS*, vol. 3, no. 5, pp. 300-305, September–October 2015, ISSN 2091-2730.

[3] Singh Inder and M. Prateek, "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma A. Hasan “A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", *IEEE International Conference on Reliability Optimization and Information Technology*, pp. 310-313, Feb 2014.

[4] N. Sharma and A. Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", *IEEE International Conference on Reliability Optimization and Information Technology*, pp. 310-313, Feb 2014.

[5] Yingbing Zhou and Yongzhen LI, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", *IEEE ICSESS*, pp. 517-520, June 2014.

[6] Ahmad, S. A., &Garko, A. B. (2019). Hybrid Cryptography Algorithms in Cloud Computing: A Review. 2019 15th International Conference on Electronics, Computer and Computation (ICECCO). doi:10.1109/icecco48375.2019.9043254.