Secure File Storage On Cloud Using Hybrid Cryptography

Aishwarya Nawal[1], Harish Soni[2], Shweta Arewar[3], Varshita Gangadhara[4]
Students, Department of Computer Engineering[1,2,3,4]
Sinhgad Institute of Technology, Lonavala, India

Abstract: *The servers that are accessed over the web and the software and databases that run on those servers are together known as "The Cloud". The amount of data needing storage is increasing every day and thus, there is a requirement for increased storage space. Cloud allows us to do the same. Storage of data on the cloud is done for various companies, colleges, for military purposes, etc. The data on the cloud is susceptible to various risks such as lack of backup services, data leakage, lack of control over your data being stored, etc. To provide a solution to these risks over cloud storage there are several ways, which include Cryptography and Steganography. Cryptography is quite popular for data security. The Cryptography technique translates original data into an unreadable form known as ciphertext. Text is converted into an unreadable form using keys. This ensures that only an authorized entity with the right key, can access the data from the cloud server. Ciphertext data is visible for everyone. There are two types of cryptography algorithms namely Symmetric Key cryptography and Asymmetric Key Cryptography. The use of a single cryptography algorithm provides basic security. In this paper, we have suggested the use of a combination of symmetric key cryptography algorithms namely: AES-GCM, Fernet, AES-CCM, CHACHA20_POLY1305 algorithm, which help to provide high-level security to the data. Here, the key is also secured using the Fernet algorithm. The file is split into N parts. Each part is encrypted simultaneously. For the file decryption purpose reverse process of encryption is applied.*

Keywords: Cloud, Cryptography, Encryption, Decryption, Security.

I. Introduction

Technological advancements are resulting in an improved standard of living. In this fast-moving life, every person uses a smartphone and has access to the internet, the major concern of people is to keep the data secure. This security concern is also about data being stored on the cloud. This concern can be taken care with the help of cryptography techniques.

The goal of cryptography is to keep the data secure from hackers or any third-party users.Non-legitimate access to data results in a loss of confidentiality. Only by taking security measures, we can stop unauthorized access or any other kind of malicious attacks on the data and also secure the user's trust in the storage of data. In the cloud computing environment, security is a crucial aspect due to important data being stored on the cloud. This data can be extremely sensitive to either an individual or a community. Hence, data management and security should be provided in such a way that users can rely on them. It is thus, imperative that the data in the cloud is protected at all costs.

So, for the security of the data present on the cloud, we have introduced a new mechanism in which we are using a combination of multiple symmetric key cryptography algorithms. In this proposed system, AES-GCM, Fernet, AES-CCM, CHACHA20_POLY1305 algorithms are used to provide security to the data. AES-GCM, Fernet, AES-CCM, CHACHA20_POLY1305 algorithms are combined to form a hybrid algorithm to accomplish high-level security to our data. The Key is also secured used Fernet algorithm.

II. Algorithms

In Symmetric Key Cryptography, both the encryption and decryption method take place using the same key.

DOI: 10.48175/IJARSCT-1101

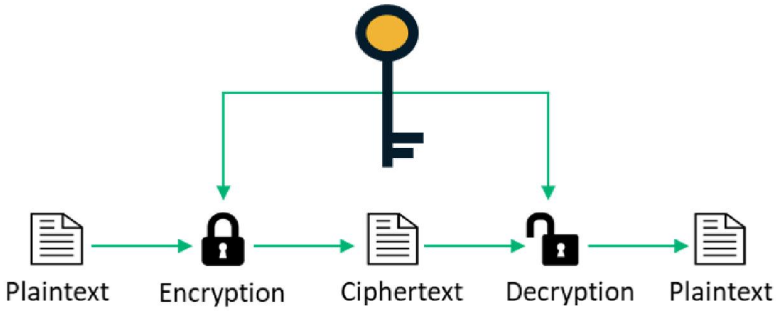

Figure 1: Symmetric Key Cryptography

2.1 AES-GCM

The combination of AES (Advanced Encryption Standard) Counter Mode encryption with Galois Hash authentication (authenticated encryption) is termed as AES-GCM algorithm. Galois/Counter Mode (GCM) is a recommended algorithm for authenticated encryption with associated data. The GCM consist block size of 128 bits which is accepted by a symmetric key block cipher, such as the Advanced Encryption Standard (AES) algorithm. Thus, GCM is considered as the mode of operation of the AES algorithm.

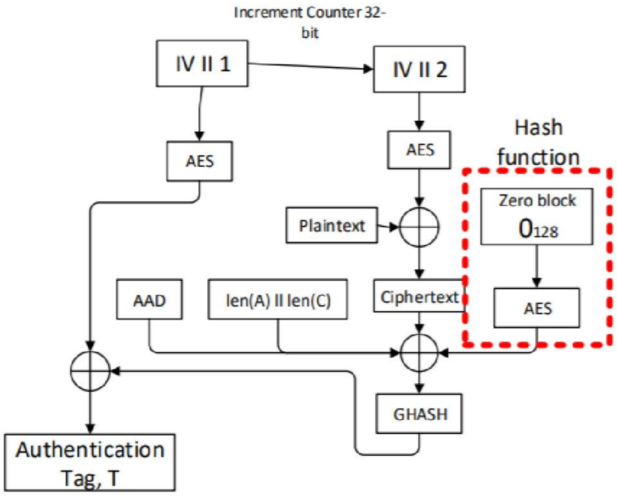

Figure 2: AES-GCM Encryption/Decryption

2.2 AES-CCM

An authenticated encryption algorithm designed to provide both authentication and confidentiality during data transfer is the basic role of CCM. It uses a 128-bit block cipher in CCM, but in this document, CCM is used with the AES block cipher. The four inputs of AES-CCM are an AES key, a nonce, a plaintext, and optional additional authenticated data (AAD). The two outputs generated by AES-CCM are a ciphertext and a message authentication code (also called an authentication tag). CCM requires two block cipher encryption operations. The nonce is generated by the authenticated encryption operation.

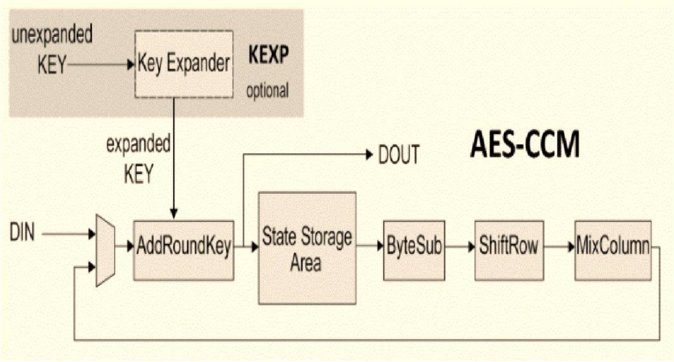

Figure 3: AES-CCM Algorithm

2.3 Fernet

The message encrypted using fernet assures us that it can't be manipulated or read without the key. Key rotation is implemented using fernet via MultiFernet. Data encrypting is done using fernet that easily fits in memory. It does not expose unauthenticated bytes in consideration of the design feature. Unfortunately, for very large files this makes it generally unsuitable. The message encrypted cannot be manipulated/read without the key as fernet is symmetric encryption. It uses URL safe encoding for the keys. Fernet makes use of 128-bit AES in CBC mode and PKCS7 padding, with HMAC using SHA256 for authentication. The IV is created from os.random(). All of these features imply the kind of thing that good software needs.

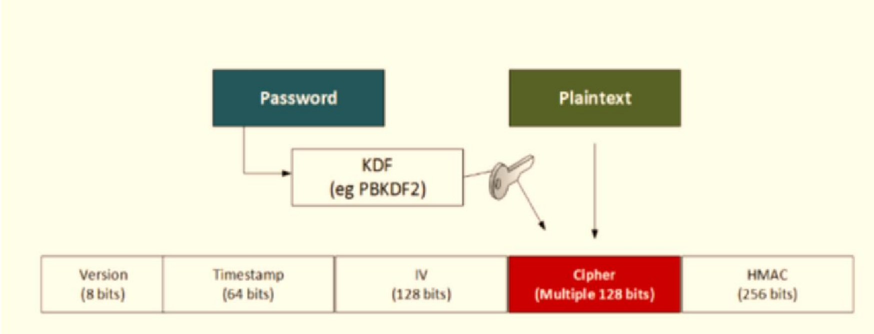

Figure 4: Fernet Algorithm

2.4 CHACHA20_POLY1305

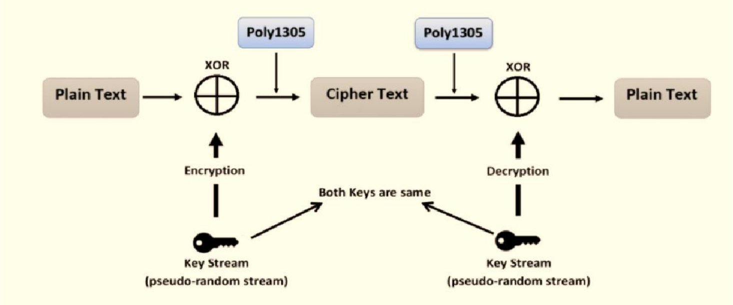

Figure 5: ChaCha20_Poly1305

It is mainly described as a high-speed cipher in [ChaCha]. It is considered to be faster than AES in software-only implementation and it is about three times faster on platforms which lack the specialized AES hardware. ChaCha20 is

DOI: 10.48175/IJARSCT-1101

also not sensitive to timing attacks. The poly-1305 is a high-level message authentication code. Its Implementation is also Straightforward and easy to get right. With an additional data algorithm, CHACHA20_POLY1305 is an authenticated encryption.

III. Proposed System

In the proposed system, a method is introduced to store the files on the cloud using hybrid cryptography algorithms. In this system, the user can both store files and also can share their files with other users in a safe manner. As these files are in the encrypted format in the cloud, only authorized users can have access to the files that are stored in the cloud.

3.1 Registration of User

Before the user can access the services that our system provides, the user must register themselves with various data like Username, Email Id, Password and Confirm Password. Once, the user register, they can go to the login page.

3.2 Login

Once the user has registered themselves with the required information, they can now login to access the services that our system grants which include: Upload files and Download of files.

3.3 Upload File

Once the user logs in, the user can perform various activities which include Uploading of their files. By uploading the files, they provide security to their data. Once the File is uploaded, encryption takes place.

For Encryption:

1. The File is loaded on the server.
2. The File is equally divided into four parts.
3. We encrypt each part using the four different algorithms. (The first part is encrypted using Fernet algorithm, the second part is encrypted using Chacha20_Poly1305, the third part is encrypted using AES-GCM, the fourth part is encrypted using AES-CCM).
4. The Keys produced while encrypting is then secured using the fernet algorithm.

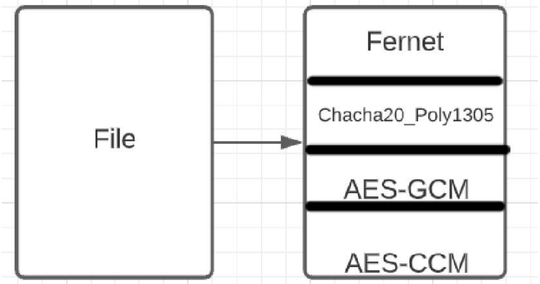

Figure 1: Splitting the file into 4 parts

3.4 Download File

Once the user logs in, the user can perform various activities which includes Downloading of various files present in the cloud. For this, the user is verified. The User who wants to download the file is asked for the name and their Email id for their verification. The details of the user-Name and email id is sent to the owner to either grant access to their files or reject it. These details are sent to the owner via Email. Once the owner grants access to user to download their file, a key is sent to the user via email.

For Decryption:

1. Load the key on the server.
2. The files which are divided into 4 parts are decrypted by when the key is entered by the user.

3. The files are then combined into a single file.
4. The file is then downloaded on the user's device.

IV. Conclusion

The main aim of this proposed system is to securely store and retrieve the data on the cloud that is only in control of the owner of the data. Cloud storage issues of security are solved using Hybrid cryptography techniques. Data security is achieved using the AES-GCM, Fernet, AES-CCM, CHACHA20_POLY1305 algorithm. Key information is secured using the Fernet Algorithm. Less time is used for the encryption and decryption process as these algorithms take minimum time and have maximum throughput for encryption and decryption. The model proposed here is a secure hybrid cryptography approach scenario to provide safe storage and safe transmission for Confidential Data files along with user authentication. In the future, we can use the proposed model to encrypt and decrypt different files such as images.

Acknowledgment

I am extremely grateful to, Principal 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 **Dr. S. D. Babar**, 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]. Jankowski, K., & Laurent, P. (2011). Packed AES-GCM Algorithm Suitable for AES/PCLMULQDQ 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.

[3]. Phan, T.-T.-D., Hoang, V.-P., & Dao, V.-L. (2016). An efficient FPGA implementation of AES-CCM authenticated encryption IP core. 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS). doi:10.1109/nics.2016.7725650.

[4]. De Santis, F., Schauer, A., &Sigl, G. (2017). ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. doi:10.23919/date.2017.7927078.

[5]. 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.

[6]. 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.