International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-1, (February 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.1.4

Hybrid Encryption using Symmetric Block and Stream Cipher

Nandinee Mudegol
Assistant Professor, Department of Computer Science and Engineering, Walchand College of Engineering, Sangli, INDIA

Corresponding Author: nandinee.mudegol@walchandsangli.ac.in

ABSTRACT

Today's digital world is entirely managed on the internet digitally. So to confirm the Confidentiality, Integrity and Availability of users data in transit and at rest using a hybrid encryption in place of using a particular encryption algorithm. In this paper we are going to propose the hybrid approach which is a combination of multiple symmetric block ciphers and stream ciphers primarily AES-GCM, Chacha20 Poly-1305, Multi Fernet and Fernet to assure more security in an acceptable time period.

Keywords-- Hybrid Encryption, Symmetric Block Ciphers, Symmetric Stream Ciphers, AESGCM, Chacha20, Poly1305, Multi Fernet, Fernet, RSA

I. INTRODUCTION

In today's technology centric world the amount of data generated is growing exponentially and so do the cyber-attacks. The major concern of the users is the end users is Confidentiality, Integrity and Availability (CIA) of the data. It can be further explained as the confidentiality of data from unauthorized access, integrity ensure the originality of data and availability states ready for operational use. There are several mechanisms used to ensure the CIA of data such as Multi-Factor Authentication (MFA), vigilance etc. to ensure security. In addition to that Data Encryption is the best practice to be followed. Encryption can be defined as a combination of several confusions (substitutions) and diffusions (replacements). It is a process of intentionally distorting data to some extent and then again transforming into another form with help of using cryptographic functions. Encryption algorithms can be broadly classified into two groups based on number of keys used:

Symmetric Encryption: In symmetric encryption the encryption and decryption of the message is performed using the same key ensuring reusability of the key.

Asymmetric Encryption: Asymmetric encryption uses two keys, for the encryption it uses a public key where as a private key used for decryption thus ensuring security.

Advantage of symmetric key encryption: Symmetric key encryption is faster as and utilizes less resources as compared to Asymmetric key encryption. And also is cost effective.

Symmetric Encryption can be further classified as block and stream cipher depending upon size of data encrypted at a time.

Stream Cipher: In a stream cipher, text is separated into small blocks, one bit or one byte long and each block is combined with a pseudorandom cipher digit stream to produce cipher text.

Block Cipher: In block cipher, text is separated into relatively large blocks and that Aach block is encoded separately. Plaintext is used during the encryption and the resulting encrypted text and ensures reliability.

Currently AES is a symmetric encryption algorithm one of the most secure and widely used. Being the strongest yet AES is also vulnerable to side channel attacks and no longer will it be required to break it completely as history suggests for several previous algorithms as DES.

We proposed a novel solution to reduce the even the slightest possibility of side channel attack by randomizing the entire encryption process, it suggests using a combination of several symmetric block and stream ciphers to encrypt data in place of a single algorithm thus assuring more security in acceptable time period. The idea is to divide the data in n fixed size parts and encrypting first k parts using k chosen algorithms, one algorithm for each part and repeating the same for remaining parts in a round robin manner. Later encrypting all the generated keys combinely using a different algorithm. The algorithms used as are follows:

For Data Encryption: AES-GCM (Symmetric Block Cipher)

Multi Fernet (Symmetric Block Cipher)

Chacha20 Poly1305 (Symmetric Stream Cipher)

For Key Encryption: Fernet(Symmetric Block Cipher)

AES-GCM [4]: Advanced Encryption Standard (AES) is a Symmetric Block Cipher used for data encryption in the proposed model. The AES has become the benchmark in encryption due to its extended implementation, efficient design, and hardware support allowing for great performance. AES-GCM is an authenticated encryption with associated data (AEAD) cipher, providing both confidentiality and data origin authentication. Galois Counter Mode (GCM) is a mode of operation for symmetric key cryptographic block ciphers. Because of its low latency and a minimum operation overhead, GCM is ideal for protecting packets of data.

Chacha20 Poly1305 [5]: Chacha20 Poly1305 an AEAD algorithm is combined mode of Poly1305 an authenticator and ChaCha20 a stream cipher. The ChaCha20 is a high-speed cipher. In software-only implementations, ChaCha20 is considerably faster than AES which is around three times faster on platforms that

lack specialized hardware for AES. The Poly1305 authenticator is designed to ensure that duplicated messages are discarded with a chances of1-n/2102.

Multi Fernet [6]: Symmetric Block Cipher mainly used for Data encryption. MultiFernet implements key rotation for Fernet which is best practice. MultiFernet offers Rotation which is a manner of cryptographic hygiene designed to restrict damage in the event of an undetected event and to increase attack difficulty.

Fernet [7]: Symmetric Block Cipher mainly used for Key encryption. Without the key, a message encrypted using Fernet cannot be read or manipulated. Fernet is a symmetric authenticated cryptography. Here GCM and Poly1305 hashing methods ensure authorization and integrity.

II. LITERATURE REVIEW

[1] Lalit Kumar and Dr. Neelendra Badal has proposed a hybrid cryptography algorithm utilizing a blend of two cryptographic strategies, viz Advanced Encryption Standard (AES) and Fully Homomorphic encryption (FHE) for cloud platforms.

[2] In this paper Vishwanath S Mahalle and Aniket K Shahade present Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud using Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES).

[3] P Shaikh, and V. Kaul displayed a hybrid encryption demonstrate utilizing a hybridization of A.E.S. and Blowfish for Confidentiality in information, Message Digest-5(MD-5) for Data dependability, Elliptic Curve Diffie Hellman Algorithm (ECDHA) for Key exchange, and Elliptic Curve Digital Signature Algorithm (ECDSA) for Digital imprint.

III. PROBLEM STATEMENT

To reduce the even the slightest possibility of side channel attack by randomizing the entire encryption process, it suggests using a combination of several symmetric block and stream ciphers to encrypt data in place of a single algorithm thus ensuring more security than current existing methodology in acceptable time period.

IV. PROPOSED METHODOLOGY

The methodology explains the process of encryption and decryption in detail.

The generic flow of the entire process is as mentioned in Fig.1.

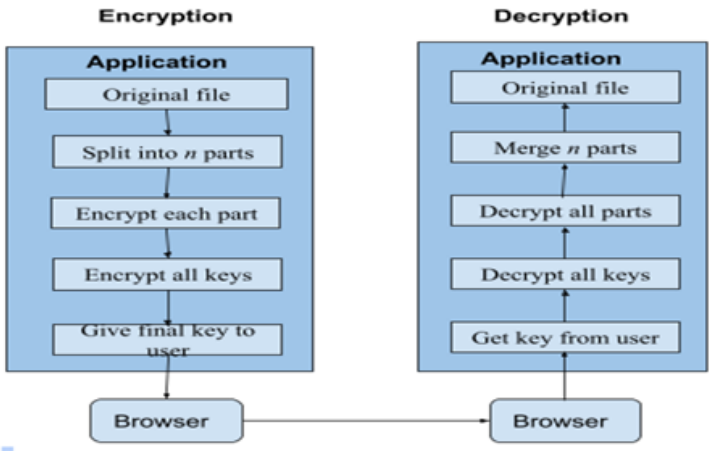

Figure 1 Proposed Methodology

4.1 Encryption

The encryption is performed using following algorithms:

For Data Encryption: AES-GCM (Symmetric Block Cipher)

Multi Fernet (Symmetric Block Cipher)

Chacha20 Poly1305 (Symmetric Stream Cipher)

k keys are generated for k data encryption algorithm and are reused in round robin fashion.

Hence, k=3.

For Key Encryption: Fernet (Symmetric Block Cipher)

Splitting. The original text file is splitted into n parts of equal size of 32 KB each. Padding is added if the last part could not make up to 32KB. A metadata file is maintained to keep a track of the original file and no. of parts made.

Data Encryption. Among the n splitted parts every k parts are encrypted with k algorithms one for each part using the k keys and the procedure is repeated for next k parts till all the n parts are encrypted, the approach followed is the round robin. Means suppose there are three algorithms, then first three parts of n parts of data are encrypted with k algorithms one by one and then the same sequence of algorithms is repeated

again for k parts of data until all the n parts are encrypted.

Keys Encryption. After performing the data encryption using k keys and k algorithms in a round manner. All k keys are combined together and encrypted using the Fernet encryption algorithm and the result is stored in a keys file.

The keys for 3 cryptography algorithms are then secured using a different algorithm named as Fernet.

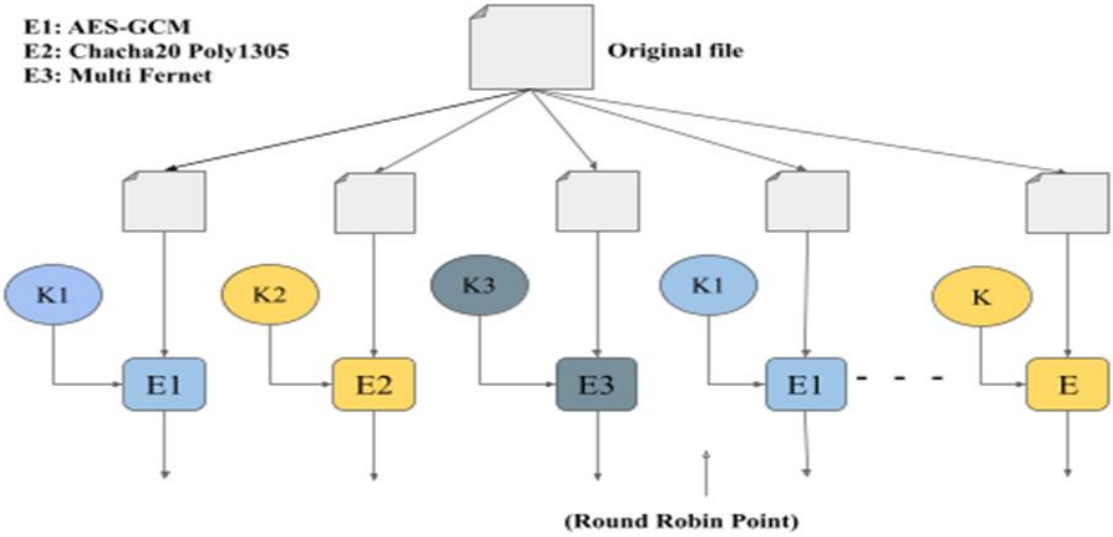

Figure 2: Splitting the files and encrypting

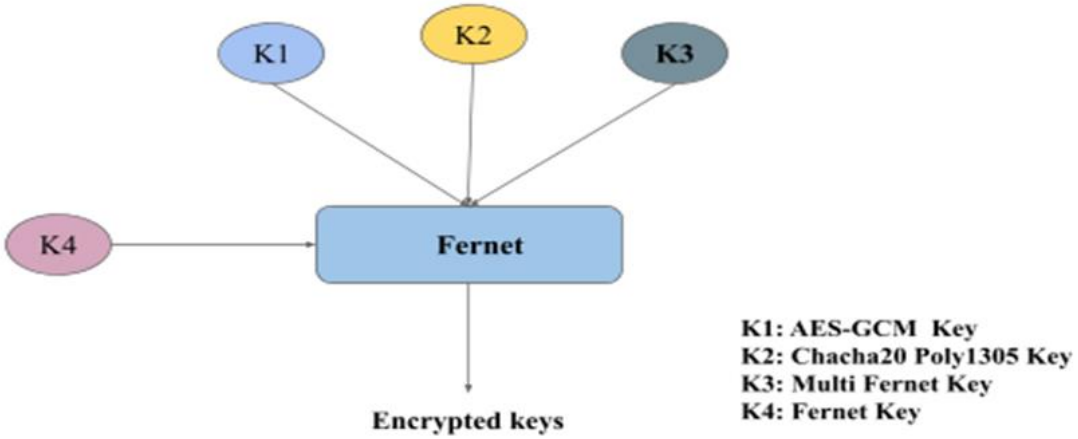

Figure 3: Combining the keys and performing encryption

The final key generated is provided to the user and is required for decryption.

4.2 Decryption

The decryption process involves the decryption of keys and then the data as follows.

Keys Decryption. The key of the fernet which has been provided to the user will be uploaded and the encrypted keys file will undergo decryption resulting in three separate keys of AES GCM, Chacha20 Poly1305 and Multi Fernet respectively.

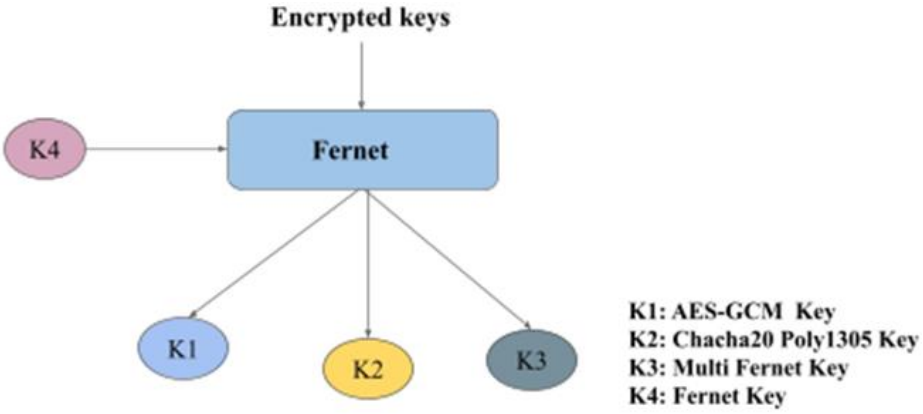

Figure 4: Performing decryption and splitting the keys

Decrypting Data. All the n encrypted parts will undergo decryption using AES GCM, Chacha20 Poly1305 and Multi Fernet respectively applied in round robin fashion using the respective decryption keys considering the manner of encryption.

Merging. After n parts are decrypted successfully, they are merged to form a single file which is nothing but the original file and it will be returned to the user.

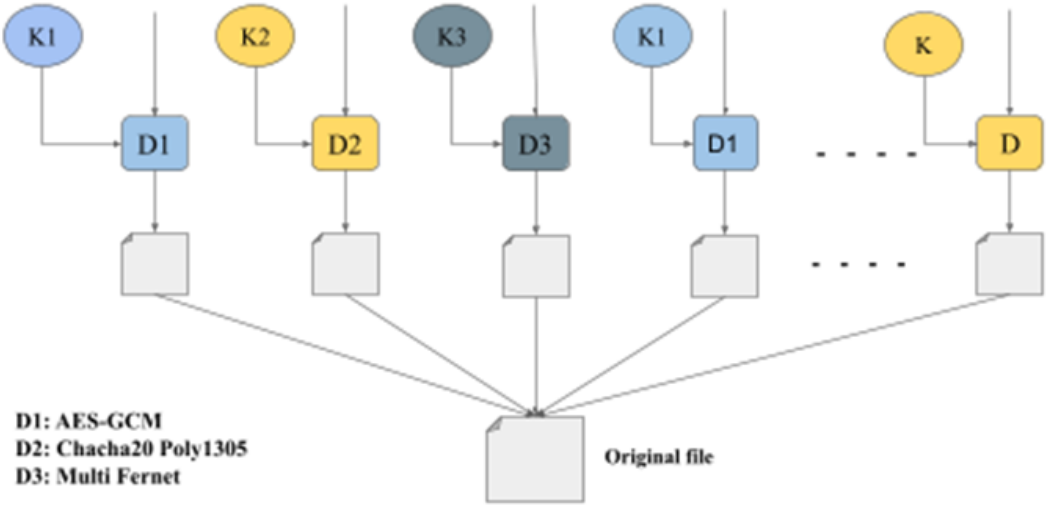

Figure 5: Decrypting the individual parts and combining to get original fileTables

V. RESULTS

Several hybrid combinations of different algorithms are implemented in order to conclude the results. The data used for encryption are plain text files of variable sizes. The hybrid combinations of algorithms used for performing analysis are categorized as follows:

5.1 Combination of only block ciphers

AES-GCM + AES-CCM

AES-GCM + AES-CCM + Multifernet

5.2 Combination of both block and stream ciphers

AES-GCM + AES-CCM + Chacha20 Poly-1305(a stream cipher)

AES-GCM + Multi Fernet + Chacha20 Poly-1305(a stream cipher)

Note: Fernet is used for keys encryption in all the cases here the primary focus is on Combination of several data encryption algorithms.

The implementation was performed on a system with 64bits processor, i5 Core, 1.70GHz CPU and 4GB RAM. The results may vary on a system with different configurations.

Following is the tabular representation of outcomes of timing in seconds (Encryption + Decryption combined)

Table 1. Block Ciphers

File Size	1) AES GCM + AES CCM (in sec)	2) AES GCM + AES CCM + Multi Fernet (in sec)
50 KB	0.062	0.056
100 KB	0.131	0.087
150 KB	0.151	0.172
200 KB	0.168	0.295
400 KB	0.501	0.639
800 KB	0.727	0.88
1 MB	1.41	1.12

Table 2. Block + Stream Ciphers

1) AES GCM + AES CCM +Chacha20 Poly1305 (in sec)	2) AES GCM + MultiFernet +Chacha20 Poly1305 (in sec)
0.049	0.052
0.086	0.091
0.136	0.139
0.189	0.183
0.324	0.306
0.619	0.608
1.042	0.946

Observations: In the case of only block cipher combinations a)-1), a)-2) the time required for encryption and decryption increases at a greater pace as the size of the file increases as compared to that of block and stream ciphers combination. Thus this choice is eliminated.

Further in block and stream cipher combination b)-1), b)-2), the combination of the AES-GCM, Chacha20 Poly-1305, Multi Fernet b)-2) performs the task in an acceptable time span even for files with larger size.

VI. CONCLUSION

The data security constraint must be ensured on every platform along with the data integrity in today's world scenario. Hence, the proposed hybrid encryption approach with extra capabilities will give a protected entry of information over the Internet. Thus helping several data centric platforms to gain the client's trust by multiplying the encryption factor. The future work includes the implementation of the model in a real time environment to encrypt the data in transit and at rest.

REFERENCES

[1] Lalit Kumar & Dr. Neelendra Badal. (2019). A review on hybrid encryption in cloud computing. *IEEE*.

[2] Vishwanath S Mahalle & Aniket K Shahade. (2014). *Enhancing the data security in cloud by implementing hybrid (Rsa & Aes) encryption algorithm*.

[3] A. P Shaikh & V. kaul. (2014). *Enhanced security algorithm using hybrid encryption and ECC*.

[4] J. Salowey, A. Choudhury & D. McGrew. (2008). AES galois counter mode (GCM) cipher suites for TLS. *Internet Research Task Force (IRTF)*.

[5] Y. Nir & A. Langley. (2015). ChaCha20 and Poly1305 for IETF protocols. *Internet Research Task Force (IRTF)*.

[6] https://cryptography.io/en/latest/fernet/#cryptography.fernet.MultiFernet.

[7] https://cryptography.io/en/latest/fernet/.