Security of Fog Storage by using Hybrid Cryptography

Kartik Singh Prajapati
M.tech Scholar
University Institute of Technology, RGPV Bhopal

Uday Chourasia
Assistant Professor
University Institute of Technology, RGPV Bhopal

Raju Baraskar, PhD
Assistant Professor
University Institute of Technology, RGPV Bhopal

ABSTRACT
Cloud has many advantages but their security is a major issue. It also has less mobility, higher time consumption in transferring data due to multihost. In our proposed system, Fog Computing(FC) is used. FC extends cloud computing services to the network edge.FC can provide more security to the cloud, their outsider sends the encrypted data to another user via fog and generates a .pem encrypted key for decryption & encryption. This key is generated by hybrid cryptography & its security is better than the existing (AES) Algorithm. Function &services of security like cryptography are loaded on fog needs which decrease storage on IoT devices & computation. The proposed system is an encryption scheme for fog IoT devices communication that used algorithms such as AES CCM, AES GCM, Fernet, Multifernet, Chacha20Poly1305is symmetric key encryption

Keywords
Fog computing; cloud computing; cryptography; security.

1. INTRODUCTION
Fog computing has many advantages such a low latency /low cost, faster than the cloud. There quick response & data transferring through edge networks and encrypted data transfer can provide security to the cloud. Cybersecurity major concern is on attackers which come forward day to day in stealing data. Nowadays, IoT devices are using in many areas & industries for automation. As digitalization emerging in the environment, brought a new attack platform on the preset menace of conventional internet. In securing IoT device-fog communication the FC can resolve distribution & resource issues.

1.1 Hybrid Cryptography
A combined public key cryptography convenience with symmetric key cryptosystems efficiency is called cryptographic system.

Public key cryptography doesn't require the receiver & sender to share the common secret in order to interface security. They are convenient, however, they often rely on complicated mathematical computation & are generally greater efficient than comparable symmetric key cryptosystem.

Any two separate cryptosystems combine to construct a hybrid cryptosystem. Cryptosystem which is a KES & DES. Encapsulation of key can be related to public-key cryptosystem & DES can be related to symmetric key cryptosystem.

1. Key Encapsulation Scheme (KES)
2. Data Encapsulation Scheme (DES)

As an example, let us assume that Nick wants to send a text message to Princy, so to encrypt the message address to Princy is a hybrid cryptosystem. Nick will do these things. First, he will get the Princy public key then he will generate a new symmetric key for the DES using a symmetric key which is just generated then he will encrypt the given symmetric key under the KES using public key of Princy and then he sends all of the encryption to Princy.

Now to decrypt the hybrid cipher text send by Nick to Princy, Princy do the following:

He uses her private key to decrypt the symmetric key contained in the encapsulations system then the message contained in the data encapsulation segment.

1.2 Problem Statement
Let's discuss, so we know that nowadays fog computing use un many areas like transportation, smart cities, surveillance, and smart buildings, and also we can retrieve data from the server on the request of the user. For storing data on fog everyone faces some major issues and also for higher security only one cryptographic algorithm is not effective to secure data in fog computing.

So the need is to use a much more complicated algorithm to improve the effectiveness of the system. Since more encryption and decryption time is needed in a single algorithm, it is not effective. Therefore data may be vulnerable to crypto attacks and also confidentiality and data integrity may be violated.

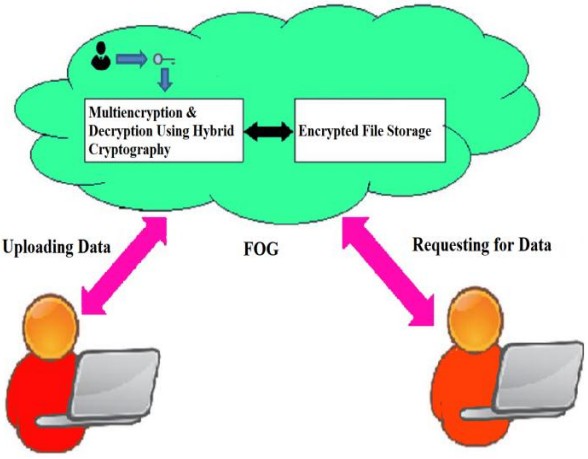

Fig 1: System overview

Above system, overview defines the system working model that how hybrid cryptography works in between different users.

In the proposed model there is a method for storing the data securely in the fog using a hybrid cryptography algorithm

2. RELATED WORK
Security is the main concern in between the privacy of users storing data on fog servers in this digital era.

V.S. Mahole & A.K. Shahade [2] also introduced a hybrid encryption scheme of AES and RSA. In their system, users create RSA Public Key & private key (RSA) where private key store with himself & uploads data with RSA public keys on the server. The server uses RSA and AES algorithm for encryption and stores data on it.

P. Uddin applied cryptography [3] in which text stenography hides information inefficiently way. With the help of public-key cryptography, stenography was proposed for pure text.which has a higher level of security.

S.D. Patil [4] system used the LSB algorithm for hiding text in the cover image and the same method for decoding. The hidden text in the mage cannot be seen with the naked eye. This algorithm used data could be stored in LSB of the title image.

S.Hesham proposed a system[5] in which she increased the efficiency of the AES Algorithm. Her method reduced delay of the critical path of 61% improvement in encryption and 29% improvement in decryption then AES system.

AES-CCM [6] acronym stands for Advanced Encryption Standard-Counter with Cipher block chaining-message authentication code.

CCM: It is generally used with a 128-bit block cipher, but here used with AES.

4 inputs: AAD(Aditional Authenticated Data), AES Key, Plaintext & a Nonce (It is created by the one who performing encryption)

2 Output: CCM output is authentication tag & ciphertext.

AESGCM [6] where GCM stands for Galois/Counter Mode. It is also a block cipher mode of generic authentication encryption.

4 inputs: Initialization Vector, AES key, AAD, and plaintext.

Output: It generates 2 outputs the same as AES-CCM.

FERNET is symmetric encryption which allows key and without key text cannot readable. It is a class in the cryptography library. It is built in many standard cryptographic parameters.

For higher security, Daniel J. Bernstein [xx] designed a cryptographic algorithm using ChaCha20 as a stream cipher and Poly1305 as an authenticator, and then software platform achieved higher performance. The amalgamation of ChaCha 20 stream cipher and Poly1305 authenticator specified by RFC7539 which made an AEAD(Authenticated Encryption with Associated Data). The applications of this are authenticity, confidentiality, the integrity of data. ChaCha20Poly1305 deployed secure & efficient. TLC connection between fog servers and IoT devices.

3. PROPOSED WORK

3.1 Objective

The aim is to have a secured platform on fog using hybrid cryptography for storing files and data. We need to use a hybrid cryptographic algorithm to maintain security. The security system is to be must sot that it should be able to reach the security necessity of the fog server and it must be robust in nature.

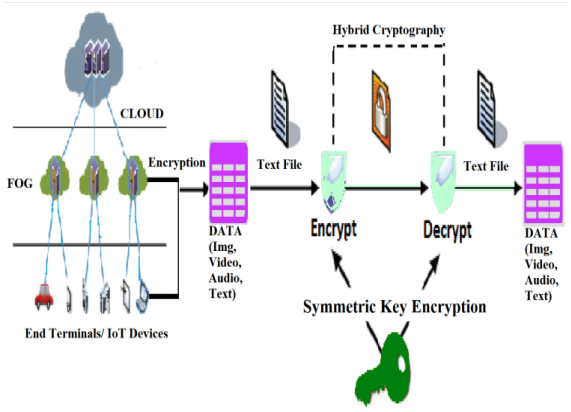

Fig 2. Proposed System architecture

In the given system the user can store data online in the fog storage and their files will bestow in encrypted format [7]. The architecture is shown above of encryption scheme used for more secured storage in fog.

3.2 Methodology

Here we have taken several cryptographic algorithms like ChaCha20Poly1305 AESGCM, Fernet, Multifernet, and AES-CCM

This algo. are used to give blockwise security to whole the data so these will be used as a hybrid cryptographic algorithm.

Here the methodology has firstly loaded the file on the server and then divide the file into n parts means file slicing is done and then any of these select above cryptographic algorithms & these algorithms can be changed with every part in a round-robin manner.

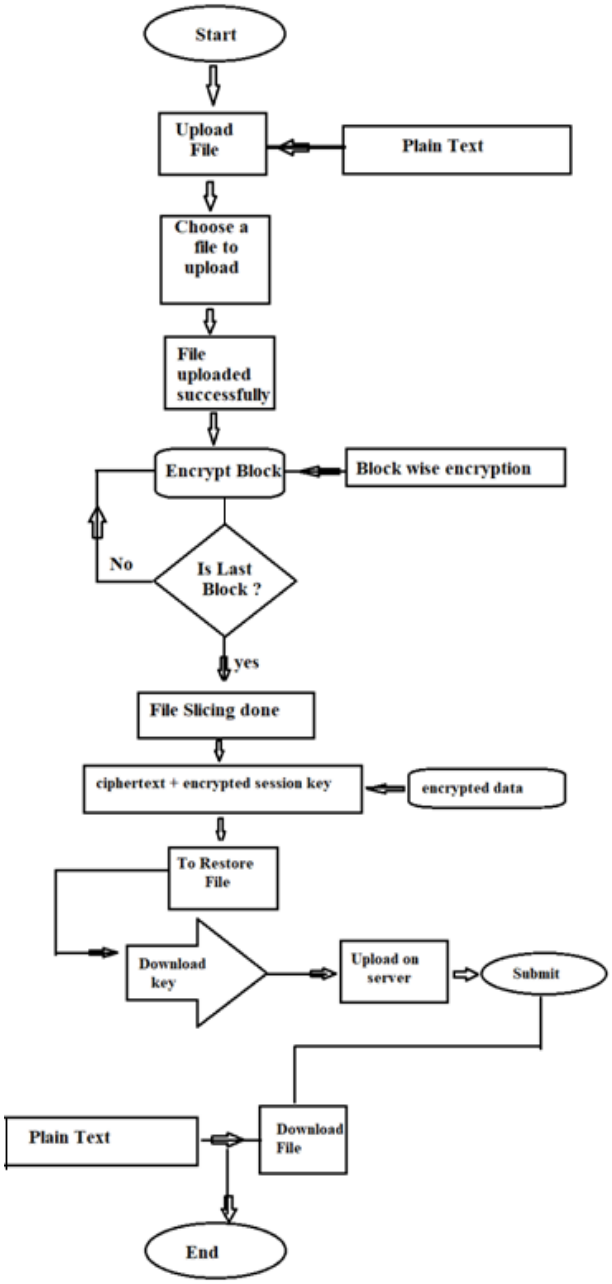

Fig 3: Flow chart of the working process

The key is for this cryptographic algorithm is then secured using the different algorithm (fernet) and the key for this algorithm is then provided to the user as a public key. Then this key will be downloaded as a public key for decrypting the files.

Now, to restore the file load the key on the server decrypt the key is of all the corresponding algorithms and the decrypted part by part and parts of the file using the same algorithms which for used to encrypt them before.

Then combine these all the n parts to form the original file and then will collect it and provide it to the user for downloading. This was the methodology used in this cryptographic system.

4. RESULT ANALYSIS

In table no. 1 symmetric key size is taken as 128kb which used in the proposed system. For different algorithms, [8] here shown that encryption time of key for the proposed hybrid cryptosystem is the least amount of time to encrypt the key.

Table1: Encryption Time is taken by 128 Kb Key

Key size in Kb	AES key encryption time in ms	Blowfish key encryption time in ms	Hybrid cryptosystem key encryption time in ms
128	3.73	3.93	1.589

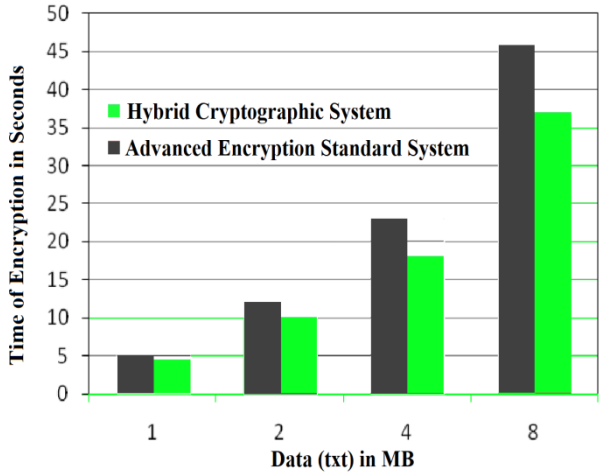

Fig 4. Encryption time compared with AES

In fig 4, we can see that the proposed cryptosystem takes less amount of count for encoding files because the proposed system is using combined symmetric key cryptography which runs continuously in a hybrid algorithm. It takes 18% to 20% lesser time as compared to the existing AES system. The single algo. can not provide higher-level privacy & security to data in fog computing.

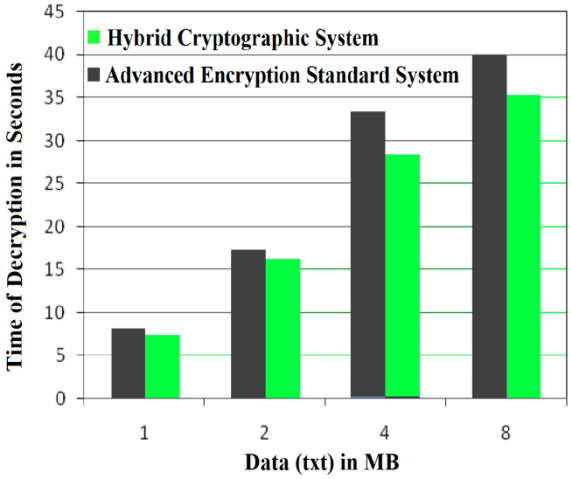

Fig 5. Decryption time compared with AES

Now, this is a new experimental result in which decryption time is shown between the AES & proposed system.

Now, we can see in figure 5, the existing AES system needs 15% - 17% more time for file (data) decryption as compared to the hybrid cryptographic algorithm. We know that, AES algo. takes the least amount of time for decryption but provides less secrecy to data.

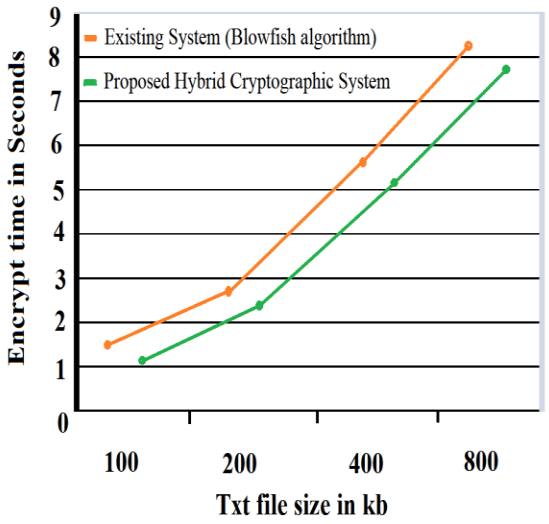

Fig 6. Encryption Time Blowfish v/s Hybrid Cryptosystem (Proposed)

Blowfish algorithm takes lesser time then AES encryption. As given in fig 6, the hybrid cryptosystem takes 13% to 15% lesser time to encode file on comparing to blowfish. The proposed system uses symmetric key so for decryption & encryption, the same key is used.

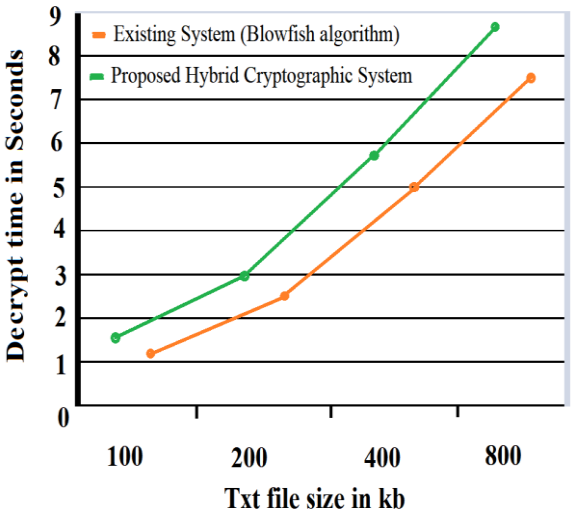

Fig 7. Decryption Time Blowfish v/s Hybrid Cryptosystem (Proposed)

In the proposed hybrid cryptosystem, the decryption time of file requires 10% - 12% less time, then blowfish. In the proposed hybrid cryptosystem, decryption time is greater then encryption time. In blowfish algo, the system takes less time for file encoding than then AES system, and for file, decryption blowfish needs more time as compared to encryption.

5. CONCLUSION

The proposed model is reliable to make the required security needs of the fog server of fog computing.

The algorithm here used like fernet, multifernet used for the encryption of the file, and as maximum throughput for encryption, decryption time from other symmetric algorithms. The idea of merging & splitting works on the principle of data security.

The hybrid approach when deployed in the fog environment makes the remote server more secure and thus fog server providers fetch more trust of the user for privacy protection & data security issue.

The fundamental challenges of detachment of access control & sensitive data are fulfilled. If this system has a disadvantage or only one disadvantage it requires an active internet connection to connect with fog server beside it has more advantages store image file is entirely secure and the file is been encrypted not by just using only one algorithm but three encryption to 4 encryption algorithm which are AES CCM, fernet, AES-GCM, multifernet. The key is also safe as it embedded the key using the other algorithm. The system is very secure and robust in nature. Data is kept secure on fog servers which prevent unauthorized access.

This system has also major applications in day to day life. The system can be implemented into banking, & corporate sectors to secure transfer confidential data.

6. REFERENCES

[1] F.De. Santis, A. Schauer, G.Sigi, "ChaCha20Poly1305 authenticated encryption for high speed embedded IoT applications", in 2017 Design Automation and Test in Europe.

[2] V.S. Mahalle, A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE, INPAC, pp 146-149, Oct. 2014.

[3] Palash Uddin, Abu Marjan, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography", IEEE, IFOST, pages 14-17, October 2014.

[4] R. T. Patil and P. S. Bhendwade, "Steganographic Secure Data Communication", IEEE, International Conference on Communication and Signal Processing, pages 953-956, April 2014.

[5] Klaus Hofmann and S. Hesham, "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170, April 2014.

[6] R. Housley, "Using AES-CCM and AES-GCM auth. Encryption in Cryptographic message syntax", in 2007 Network Working Group.

[7] Neha Shrikant Dhande, FOG COMPUTING: REVIEW OF PRIVACY AND SECURITY ISSUES, International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015.

[8] M. N Wahid, A. Ali, B. Esparham, M. Marwan," Comparison of crypto. Algo: DES, 3DES, AES, RSA & blowfish for guessing attacks prevention" in 2018 Comp Sci Appl Technol