International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Secure File Storage on Cloud Using Hybrid Cryptography

Prof. Gajanan Tikhe[1], Shivani Jayde[2], Harish Gaurkhede[3], Ruchika Vaidya[4], Anjali Wankhade[5], Vaishvani Yelekar[6]

[1]Assistant Professor, Dept. of Computer Science & Engineering, Datta Meghe Institute of Engineering Technology & Research, Wardha, Maharashtra, India
[2-6]Student, Dept. of Computer Science & Engineering, Datta Meghe Institute of Engineering Technology & Research, Wardha, Maharashtra, India

---

Abstract - Our main aim in this project is to store the information securely on the cloud storage, by splitting the data in different chunks and storing those parts of data on cloud in such a manner that preserves data confidentiality, integrity and ensures availability. The usage of cloud computing is rapidly increasing in so many organizations and IT industries are providing new software's with minimum cost. Cloud computing is helpful in terms of low cost and accessibility of information. Cloud computing provides with a lot of features with low cost and of knowledge accessibility by using Internet. To ensure the protection of data, cloud computing can play a major role, as the users usually store their sensitive information on the cloud, but these providers are also unknown and untrusted. So, the most challenging issue is to share the data in secure way while preserving that data from any untrusted cloud. Our approach ensures that protection and privacy of client's important information by storing the client's data on any single cloud by using AESCCM, AESGMC and Chacha20poly1305 algorithms.

1.INTRODUCTION

Cloud storage enables you to store your data on hosted servers. There is a huge risk of data misuse, when different organizations implement the use of the cloud to save their data. To avoid any such risk and to secure the user data, there is an urgent need to secure the data repositories. Since, sensitive data is present on the cloud there is a need to protect this data from Unauthorized Access.[1] This Security concern of protecting the data from Unauthorized access can be solved using various ways, the most commonly used techniques are cryptography. [6]

1.2 PROBLEM STATEMENT

The customers who store their data with cloud service providers are liable to several threats. In our work, we have considered four different varieties of threat models. First, the single point of failure, which affects the information availability that would occur in case if a server of any cloud service provider has failed. Information availability is again a crucial issue which can also be affected, if in case the cloud service provider i.e., CSP, has run out of the service. [1]

Secondly, one major threat is data integrity. Integrity can be a degree of confidence that the information within the cloud that is what's imagined to be there, and has the protection against any accidental or intentional changes without proper authorization. Such worries are always present; so, in that case, a cloud service's customer cannot completely rely upon a cloud service provider to ensure the proper storage of his important data. [2]

Security is a very necessary service for any network whether wired or the wireless network communication for enhancement of what was offered by the cloud. Simply by only storing the information and knowledge on clouds does not solve the matter. The matter isn't about data availability, but about the security of information. The characteristic of this method is that the key requires to be joined by reconstruction.[7] Many of the companies that have not adopted the cloud platform because of the fear of getting their data leaked. This is related from the very fact that the cloud is a multi-user environment, in such a case all the resources are shared. It is a third-party service, which implies that the data can be in potential danger of being viewed or mishandled by the provider. It is the only attribute on which we can doubt the capabilities of a third-party, which is looking like a very big risk when it is involving various different businesses and those businesses sensitive business data.[2] There are also different variety of external threats which could cause data leakage, that includes the malicious hacks of cloud providers or it can compromise data of cloud user accounts. The simplest strategy for this is to depend upon a file encryption system which provides stronger passwords, rather than completely trusting and depending on the cloud service provider themselves. [3]

1.3 OBJECTIVES

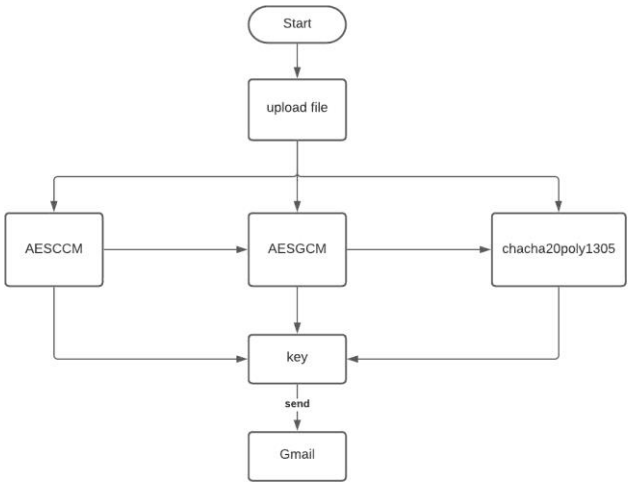
1. To achieve the secure file storage on the cloud using hybrid cryptography.

2. In case of data security and privacy protection problems, the basic challenge of segregation of important data and access control is fulfilled.

2. ARCHITECTURE

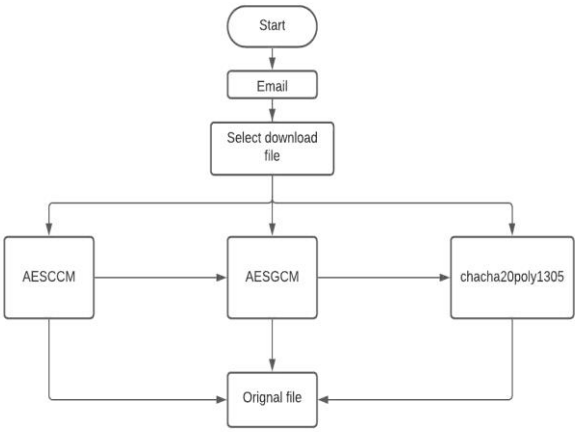
Encryption:

The subset of the Rijndael cipher which is developed by the Belgian cryptographers is AES, Vincent Rijmen and Joan Daemen, who submitted the proposal to NIST during the AES selection process. Rijndael is the family of ciphers with different key and block sizes. For AES, NIST selected each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

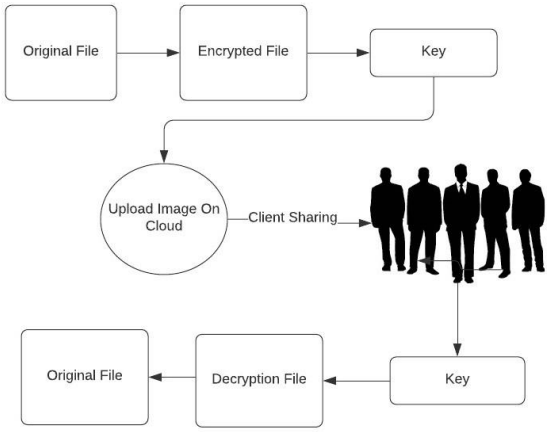


Decryption:

One of the explanations for implementing data travels over the net, it becomes very important to do scrutiny of the access from unsanctioned organizations. Due to this, the information is encrypted so as to reduce the data loss and theft of data. Common type of files is encrypted including images, text files, e-mail messages, user data and directories. The user who is recipient of decryption receives a prompt or such a window on which a password is to be entered to access the encrypted data. For the decryption process, the system extracts and converts the encrypted data and changes that data into words and pictures which are easily understood by any reader and by any system. This process can be done either manually or automatically. Decryption can be performed with the help collection of keys or passwords.



2.2 SYSTEM ARCHITECTURE



3. METHODOLOGY

3.1 MODULE DESCRIPTION

Here we've taken several cryptographic algorithms like ChaCha20Poly1305 AESGCM, Fernet, Multifernet, and AESCCM This algorithm are wont to give block wise security to whole the info so these are going to be used as a hybrid cryptographic algorithm.[3]

Here the methodology has firstly loaded the file on the server so divide the file into n parts means file slicing is finished then any of those select above cryptographic algorithms & these algorithms are often changed with every part in an exceedingly round robin manner.[4]

AESCCM Algorithm

- CCM mode could be a mode of operation for cryptographic block ciphers. This is an authenticated encryption algorithm which is designed for producing both authentication and confidentiality. CCM mode has been just defined for block ciphers and AES-CCM

has four inputs. They are AES key, a nonce, a plaintext, and finally an optional additional authenticated data with a block length of 128 bits. AES-CCM algorithm generates two outputs: a message authentication code which is also called an authentication tag and a ciphertext. [5]

AESGCM Algorithm

- The Galois/Counter Mode (GCM) is specified in [GCM]. GCM is a generic authenticated encryption block cipher mode. GCM is defined for use with any 128-bit block cipher, but in this document, GCM is used with the AES block cipher. AES-GCM has four inputs: an AES key, an initialization vector (IV), a plaintext content, and optional additional authenticated data.
  AES-GCM generates two outputs: a ciphertext and message authentication code.[4]

ChaCha20Poly1305Algorithm

- ChaCha could be a stream cipher supported a 512-bit ARX hash function in counter mode. ChaCha doesn't use S-Boxes. It's fast and constant-time without hardware acceleration. ChaCha20 is ChaCha with 20 rounds. ChaCha nonces are 24 bytes, which allows you to come up with them randomly and not worry a few birthdays collision until about 2^ messages (for the identical collision probability as AES-GCM).

  - Poly1305 uses different 256-bit key for every (nonce, key) pair. ChaCha20-Poly1305 uses the primary 16 bytes of the nonce and therefore the 256-bit key to come up with a definite subkey, then employs the quality ChaCha20-Poly1305 construction employed in TLS today. For application-layer cryptography, ChaCha20-Poly1305 contains most of the properties you'd want from an authenticated mode.[3]

4. OUTPUT/RESULT

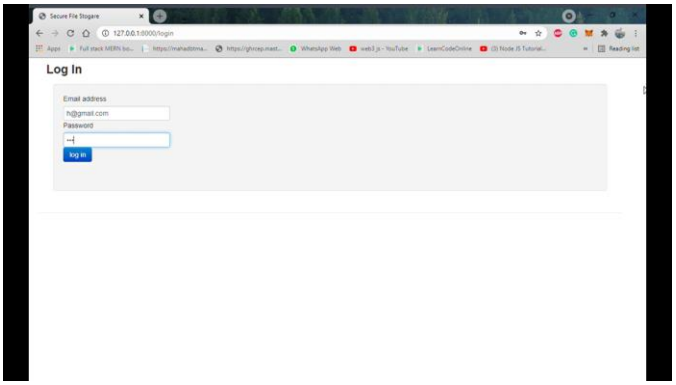


Fig 4.1: Screenshot1

In **Screenshot 1,** we are representing the module 1 which is registration page & login page. For the secure authentication we have to register with a email-id & a strong secure password.

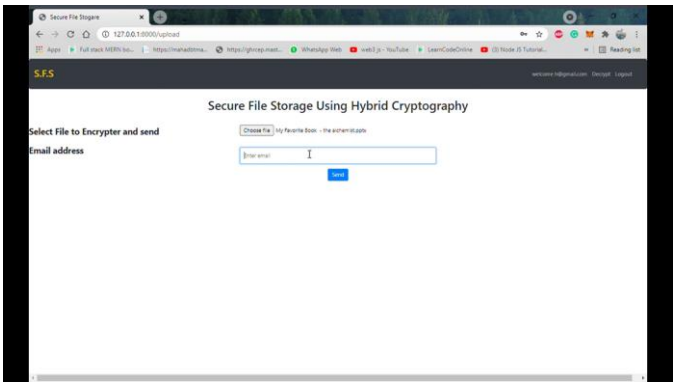


Fig 4.2: Screenshot2

In **Screenshot 2**, we have Encrypt the data here, firstly select the file which we want to encrypt & then write email address of whom we send the encrypted file & click the send button.

Fig 4.3: Screenshot3

In **Screenshot 3,** we have successfully encrypted file in the form of combination of public key & private key by using three algorithms, & successfully send on receiver's Gmail.

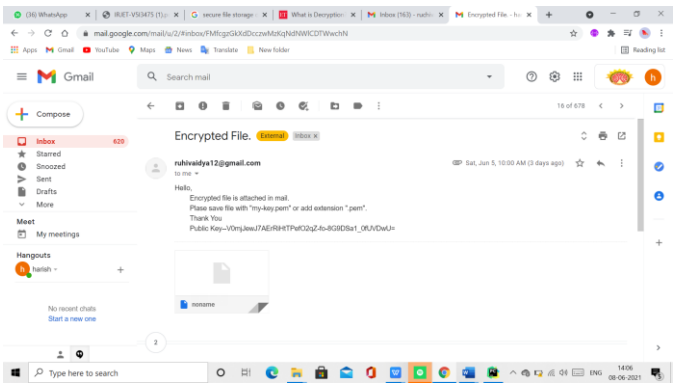


Fig 4.4: Screenshot4

In **Screenshot 4** this is receiver's email-id, here we able to see that, receiver have an email which is included by encrypted file which we had send to the receiver. Download this file with ".pem".

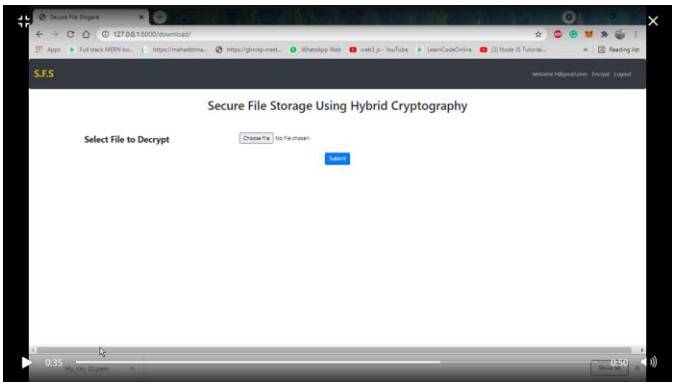


Fig 4.5: Screenshot5

In **Screenshot 5,** The Encrypted file which we downloaded from the receivers. Select here for the decryption.

In **Screenshot 6,** we have successfully decrypt, encrypted file by using three algorithms, & here we have our original file which is send by a sender.

5. CONCLUSIONS

- Cloud is able to handle the longer-term requirements for accessing multimedia files thanks to limited capabilities of low configured devices available. But the cloud and its users have many privacies and security related aspects that needs special attention.
- Data security and privacy protection are the first problems that require to be solved. The model proposed here could be a secure hybrid cryptography approach scenario to supply a secure storage and safe transmission for Confidential Data files.
- The fundamental challenges of detachment of access control & sensitive data are fulfilled.
- If this technique features a disadvantage or only 1 disadvantage it requires an energetic internet connection to attach with server beside it's more advantages store image file is entirely secure.
- the file is been encrypted not by just using just one algorithm but three encryptions to 4 encryption algorithm which are AES CCM, fernet, AES-GCM, multifernet.
- The secret is also safe because it embedded the key using the opposite algorithm. The system is very secure and robust in nature.
- Data is kept secure on servers which prevent unauthorized access.
- This system has also major applications in day-to-day life. The system will be implemented into banking, & corporate sectors to secure transfer confidential data.

REFERENCES

[1]] 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.

[2] 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 Techno.

[3] Radu Iacomin, Stock market prediction "2015 19th International Conference on System Theory, Control and Computing (ICSTCC)".

[4] Ko Ichinose Stock market prediction from news on the Web and a new evaluation approach in trading "2016 5th IIAI International Congress on Advanced Applied Informatics".

[5] Ashish Sharma, Dinesh Bhuriya, Upendra Singh Survey of stock market prediction using machine learning approach "2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)".

[6] Mr. Gajanan N. Tikhe, Mr. Jeetendra Ambulkar, "A Certificate-Based Scheme to Defend against Worm hole Attacks in Ant based Adaptive Multicast Routing protocol for MANET", in ICCCT, Delhi on 6th August 2011

[7] Mr. Gajanan N. Tikhe, Mr. Yogadhar Pandey, "A Secure Scheme to Avoid Worm hole Attacks in Ant based Adaptive Multicast Routing protocol for MANET", IFRSA's INTERNATIONAL JOURNAL OF COMPUTING (IIJC) Volume 2, Issue 1, ISSN (Print):2231:2153, ISSN (Online):2230:9039, Jan 2012