JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

STUDY ON SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

[1]Aishwarya Bawane, [2]Radhika Gourkar, [3]Sonia Mondal, [4]Shruti Khanke, [5]Rupa Lichode

[1,2,3,4] B.Tech students, department of CSE, Rajiv Gandhi College of Engineering, Research and Technology, Chandrapur, India
[5]Assistant Professor, department of CSE, Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, India

Abstract : In this paper we aim to securely store information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that preserve data confidentially integrity and ensures availability. The rapidly increased use of cloud computing in the many organization and IT industries provides new software with low cost. Cloud computing is beneficial in terms of low cost and accessibility of data. Cloud computing gives lot of benefits with low cost and of data accessibility through internet. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers may be untrusted, So sharing data in secure manner while preserving data from an untrusted cloud is still a challenging issue. Our approach ensures the security and privacy of client sensitive information by storing data across single cloud, using AES, 3DES and Blowfish algorithm.

Keywords—Cloud Computing, Cryptography, Hybrid Cryptography, File Storage, AES, 3DES, and Blowfish Algorithm

I. INTRODUCTION

How the system is secured? Files storage in cloud using hybrid cryptography works. Now a days cloud computing is using may areas like industries, military, colleges, etc. to store huge amount of data. You can retrieve the data from cloud and request us to user that security of file stored on cloud server is very less. Sometimes a single technique or algorithm alone cannot provide high-level security. To provide the solution of the issuethe approach used in this project is Hybrid Cryptography Technique which includes AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard) and Blowfish Algorithm.

How cloud storage works it stores the users' confidential files on the storage servers, and users have the freedom of accessing their files from any location. All of a user's devices such as tablets, laptops, mobile phones, desktop PCs and other technology gadgets can be used to store and access files stored on the cloud. Businesses can also benefit from cloud storage by being able to improve productivity considerably with the help of cloud storage. Cloud storage thus eliminates the need for carrying physical storage devices.

The new security mechanism using symmetric key cryptography algorithm. File security concerns arise because both user's application and program are residing in provider premises. The cloud provider can solve this problem by encrypting the files by using encryption algorithm. A file security model to provide an efficient solution for the basic problem of security in local system environment. Hybrid encryption is used where files are encrypted by three algorithms coupled with file splitting which is used for the secured communication between users and the servers. Data security use of single algorithm is not effective for high level of security to data in cloud computing. AES, 3DES and Blowfish algorithms are combined to form a hybrid algorithm to accomplish better security. It makes it difficult for the attacker to recover the secret file of the user.

I. TIMELINE FOR FILE STORAGE

1956	IBM Ships 1st HARD DRIVE-**5MB Size** of 2 Refrigerators
1971	First FLOPPY DISK-STORE 80KB, **READ ONLY 1st read/write floppy released** by Memorex in 1972
1980	World First 1GB + HARD DRIVE Cloud store 2.52 GB. Size of 1 refrigerator
1985	First CD-ROM Can store up to **900MB**
1996	First DVDS Stores **4.7GB** of data
2001	First USB FLASH DRIVE, **Stored 8MB Modern flash drives can store upto 128GB**
2006	AMAZONS ELASTIC COMPUTE CLOUDE(EC2)**CLOUD SERVICES** now offer as much offsite storage as an individual or company
2007	HITACHI: FIRST 1 TERABYTE (1024GB) **HARD DRIVE**
2011	1.8 ZETABYTES(1.8 TRILLION GBS) OF DATA CREATED IN 2011 (enough to build a great ipad wall of china, twice as tall as the origanl)
2012	DATA COLLECTION VOLUME INCREASED BY 400% IN 2012
2013	**CLOUD ESTIMATED TO CONTAIN MORE THAN 1 EXABYTE OF DATA**
2014	**COMPANIES CAN NOW ANALYSE PETABYTES OF DATA- 20M FOUR DRAWER FILING CABINETS OR 13.3 YEARS OF HDTV**
2018	**AMOUNT OF DATA ON INTERNET 40 TIMES LARGER THAN 2009**
2020	**1/3 OF ALL DATA** will have passed through the cloud, we will have created35 ZETABYTES OF DATA

II. Data Security Issues

Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for application and data in cloud. Some of the issues are as following:

- Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a particular resource that has been compromised.
- According to service delivery models of cloud computing, resources and cloud services may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.
- Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

III. Hybrid Cryptosystem

Hybrid Cryptography concept is used for securing storage system of cloud. Two different approaches are used to show the difference between less secure and more secure systems. The first approach is using AES algorithms for encrypting the file. After encryption the received text is a cipher text is going to encrypt again for second time either 3DES or blowfish depends upon file size. If the file size is more than 100 characters it will be the 3DES algorithm and if the file size is less than 100 characters then it will be using blowfish algorithm.

Algorithm Used

1. **Advanced Encryption Standard (AES):**

The Advanced Encryption Standard (AES) also known as 'Rijndael' is a symmetric-key block cipher algorithm having three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits respectively. The AES algorithm has maximum block size of 256 bits whereas Key size is unlimited. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network, thus making it stronger and faster than Triple-DES.

Step-wise description of the algorithm:

Key Expansions:

Round keys are derived from the cipher key using AES key schedule, it also requires a separate 128-bit round key block for each round plus one more.

Initial Round:

Add Round Key - using bitwise xor each byte of the state is combined with a block of the round key.

Rounds:

(a) Sub Bytes - according to a lookup table each byte is replaced with another in a non-linear substitution step.

(b) Shift Rows - a transposition step where the last 3 rows of the state are shifted cyclically a certain number of steps.

(c) Mix Columns - a mixing operation which operates on the columns of the state, combining the 4 bytes in each column.

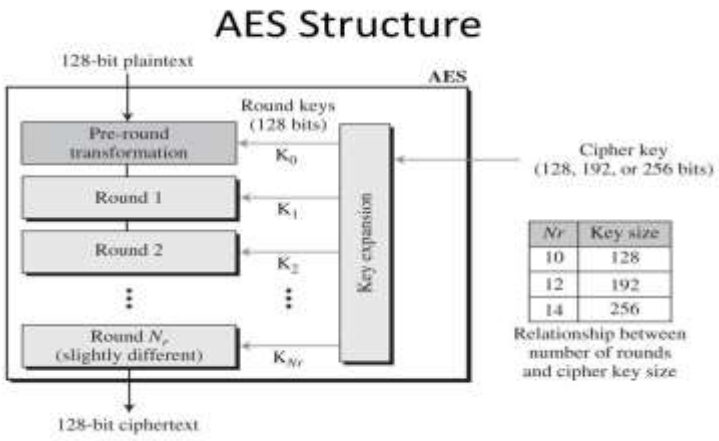
(d) Add RoundKey

Final Round (no Mix Columns)

(a) Sub Bytes

(b) Shift Rows

(c) Add Round Key.



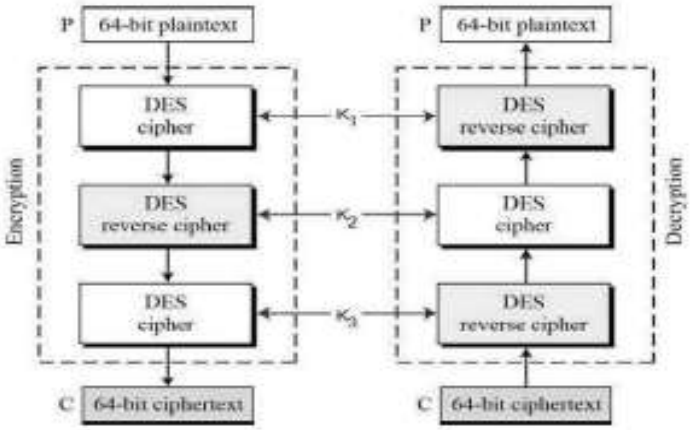
2. Triple Data Encryption Standard (3DES)

In cryptography, 3DES is an inherited enhanced version of DES (Data Encryption Standard). In the Triple DES algorithm, DES is used trice to increase the security level. Triple DES is also referred to as TDES or Triple Data Encryption Algorithm (TDEA).

TDES has following key:-

- All keys being different
- Key 1 and key 2 being different & key 1 and key 3 is the same.
- All keys being identical

TDES is slowly invisible from use, it is maximally replaced by the AES (Advanced Encryption Standard). A far-reaching anomaly is in the digital payments industry, which still uses 2TDES and scatters standards on that basis (e.g. EMV, the standard for interoperation of "Chip cards", and IC capable POS terminals and ATM's). This guarantees that TDES will remain as an agile cryptographic standard in the future.



Triple DES Procedure

3. Blowfish Algorithm

Blowfish is a symmetric block cipher which uses a Fiestal network, 16 rounds of iterative encryption and decryption functional design. The block size used is of 64-bits and key size can vary from any length to 448.Blowfish cipher uses 18 sub arrays each of 32-bit commonly known as P-boxes and four Substitution boxes each of 32-bit, each having 256 entries. The algorithm design is shown in figure. It consists of two phases: one is Key Expansion phase another is Data Encryption phase. In Key expansion phase, key is converted into several sub-keys and in Data Encryption phase, encryption occurs via 16-round networks.
Each round consists of a key dependent permutation and a key and data dependent substitution.

IV. PROPOSED SYSTEM

Selectively sharing data files on the cloud becomes a burden on the data owner as the hierarchy grows (the access privileges increase in number) and/or as the access restrictions become more complex due to an increase in the sensitivity of the file segments. A trivial solution involves the data owner to use public key encryption. This solution would require the data owner to encrypt the same part of the data file once for each data user being granted access then upload the resulting cipher texts to the cloud. The data users would then fetch their uniquely encrypted parts of the file from the cloud and utilize their private keys to decrypt them. This method ensures that no unprivileged data user will gain access to any part of the data file even if that user is able to download the cipher texts from the cloud. However, on a large scale, public key encryption becomes an inefficient solution due to the increase in the number of encryptions and large storage spaces required. Therefore, the challenge is to provide the data owners with an efficient, secure and

privilege-based method that allows them to selectively share their data files among multiple data users while minimizing the required cloud storage space needed to store the encrypted data segments.

• Requiring less network communication.
• We present multiple data file partitioning techniques and propose a privilege-based access structure that facilitate data sharing in hierarchical settings.
• A new security layer is added to encrypt the data of the task before transferring to the cloud side by using AES and Triple DES encryption technique.

V. DESIGN AND IMPLEMENTAION

Cloud proprietor transfer the information on cloud worker. Record is part into octet. All aspects of document are encoded all the while utilizing multithreading strategy. Encoded record is put away on cloud worker. Keys utilized for encryption are put away into cover picture. Distributed computing is the multi-client climate. In this beyond what one client can get to record from cloud worker. Cloud client demand for file. On solicitation of record client additionally get steno picture utilizing email which comprise of key data. Switch measure is utilized for translate the document.

MODULES

- DATA OWNER
- DATA USER
- ADMIN
- CLOUD

- **DATA OWNER (DO)**

Owner upload the data on cloud server. File is split into octet. Every part of file is encoded simultaneously using multithreading technique. Encoded file is stored on cloud server. Keys used for encryption are stored into cover image. Cloud computing is the multi user environment.

- **DATA USER (DU)**

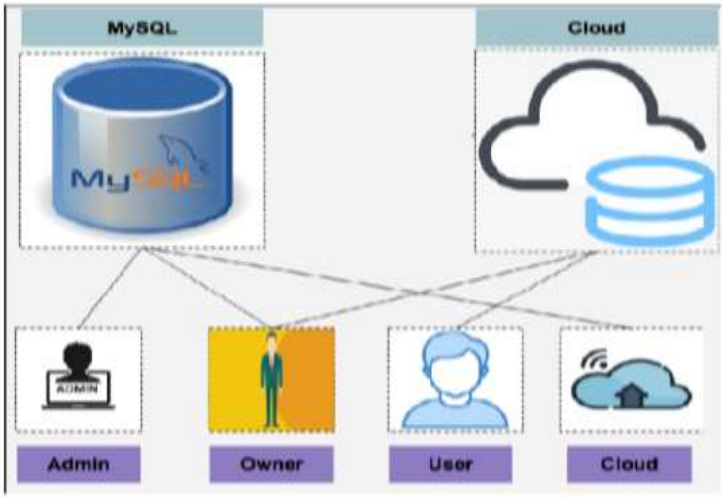
Cloud user request for file. On request of file user also get key using email which consist of key information. Reverse process is used for decode the file.

- **CLOUD**

Cloud module can operate by the admin in cloud module having all the registered users, owner details and owner uploaded file details and user uploaded file details.

- **ADMIN**

Admin login with username and password, the entered username and password is correct then only admin enter into the home page, if entered details are incorrect admin can't login to home page, after entered into the home page admin act like owner of this application and admin activate and deactivate the user and owner of this application and admin activate and deactivate the user, owner and admin can view all uploaded file details and request details.



System Architecture

VI. CONCLUSION

This project implements a double stage encryption algorithm that provides high security, scalability, confidentiality and the easy accessibility of multimedia content in the cloud. The proposed algorithm is crucial in the second stage, the randomly generated key provides more security than the conventional encryption system. The ciphertext is stored in the cloud instead of original multimedia content. The cipher text is undoubtedly hard to recover the original content for random asymmetric key. Wide application of the proposed algorithm protects the information from the side channel attacker to grab the multimedia data from the cloud. Thus, the multimedia content is safe in the cloud.

VII. REFERENCES

- A Hybrid Cryptography Algorithm for Cloud Computing Security, International journal of Core Engineering & Management – 2017.
- Hybrid Cryptography Algorithms in Cloud Computing: A Review, 15th International Conference on Electronics Computer and Computation ICECCO – 2019.
- Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language". IEEE Transactions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.
- Kumar, A., Lee, B. G., Lee, H., &Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).