IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure File Storage on Cloud Using Hybrid Cryptography Algorithm

1.Uttam Kumar 2. Mr. Jay Prakash

1 Student, School of Computing Science and Engineering, Galgotias University, Uttar Pradesh,

2Assistant Professor, School of Computing Science and Engineering, Galgotias University, Uttar Pradesh,

Abstract —

Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security. This Security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So we have introduces a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric key and steganography. In this proposed system 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES (Advanced Encryption Standard) algorithms are used to provide security to data. All the algorithms use 128-bit keys. LSB steganography technique is used to securely store the key information. Key information will contain the information regarding the encrypted part of the file, the algorithm and the key for the algorithm. File during encryption is split into three parts. These individual parts of the file will be encrypted using different encryption algorithm simultaneously with the help of multithreading technique. The key information is inserted into an image using the LSB technique. Our methodology guarantees better security and protection of customer data by storing encrypted data on a single cloud server, using AES, DES and RC6 algorithm.

Keywords— Cloud Computing and Storage, AES Algorithm, RSA Algorithm, Blowfish Algorithm

Introduction-

Cloud computing is originated from earlier large-scale distributed computing technology. NIST defines cloud computing as a model for enabling convenient on demand network access to a shared pool of configurable computing resources (like network, storage, application and services) that can be quickly provisioned and released with minimal management effort or service provider interaction.

In Cloud computing files and software are not fully contained on the user's application and Program are residing in provider premises. The cloud provider can solve this problem by encryption the files by using encryption algorithm. This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid encryption is used where files are encrypted by file splitting and RSA is used for the secured communication between users and the servers.

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.

Hybrid Cryptosystem Scheme

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 uses RSA and AES algorithms; RSA is used for key encryption and AES is used for text or data encryption. In the second or we can say more secured approach, AES and Blowfish algorithms are used. In this approach, these two algorithms provide double encryption over data and key which provides high security compared to the first one.

I. In this proposed system three step procedures is used. Firstly, Diffie Hellman is used for exchanging keys. Thereafter authentication is performed using digital signature scheme. Finally, data is encrypted using AES and then uploaded to the required cloud system. For decryption reverse procedure is implemented.

II. Combination of RSA algorithm and MD5 to assure various security measures such as confidentiality, data integrity, no repudiation etc. It uses RSA key generation algorithm for generation of encrypted key for encryption and decryption process. MD5 digest is used for accepting an input of length up to 128 bit and processing it and generating an output of padded length for encryption and decryption process.

III. Implementation of Trusted Storage System using Encrypted File System (EFS) and NTFS file system drive with help of cache manager for securing data files. EFS encrypt stored files by automatically using cryptographic systems. The process takes place as follows, firstly application writes files to NTFS which in turn places in cache and return backs to NTFS. After this NTFS asks EFS to encrypt files and heads them towards the disk.

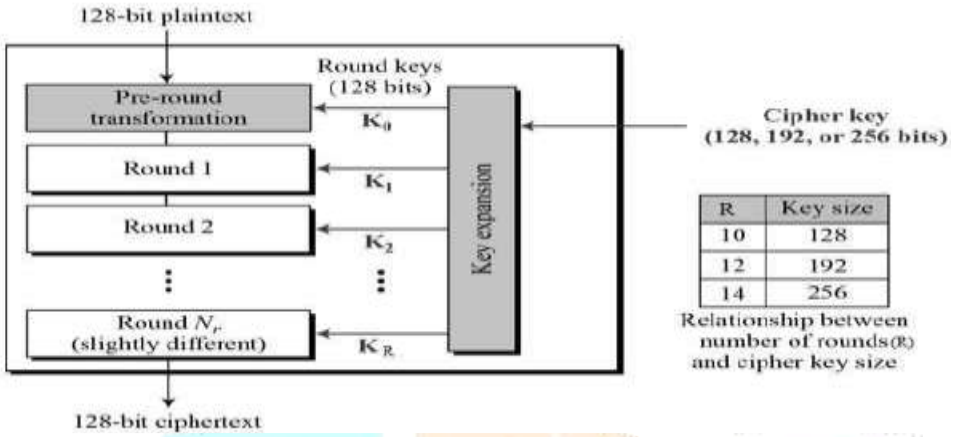
IV. Cloud Storage Security Service is provided by using separate servers viz. User Input, Data Storage and User Output. Three different servers are used to ensure that failure of any of the servers doesn't harm the data. User Input server is used for storing user files and input data by providing user authentication and making sure the data is not accessed by any of the unauthorized means. Data storage server is the place where the encryption using AES is performed to secure user input and then the encrypted files are transferred to User Output server. User Output Server is the place from where user gets the output file or the decrypted file and uses it for further use.

Algorithm Used

Advanced Encryption Standard (AES)

The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continue serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of bits (permutations).

All AES calculations algorithm is executed in bytes instead of bits. Therefore, for Advanced Encryption Standard, 128 bits of plain data is considered as a block of 16 bytes These 16 bytes are arranged in a 4x4 matrix for the processing.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

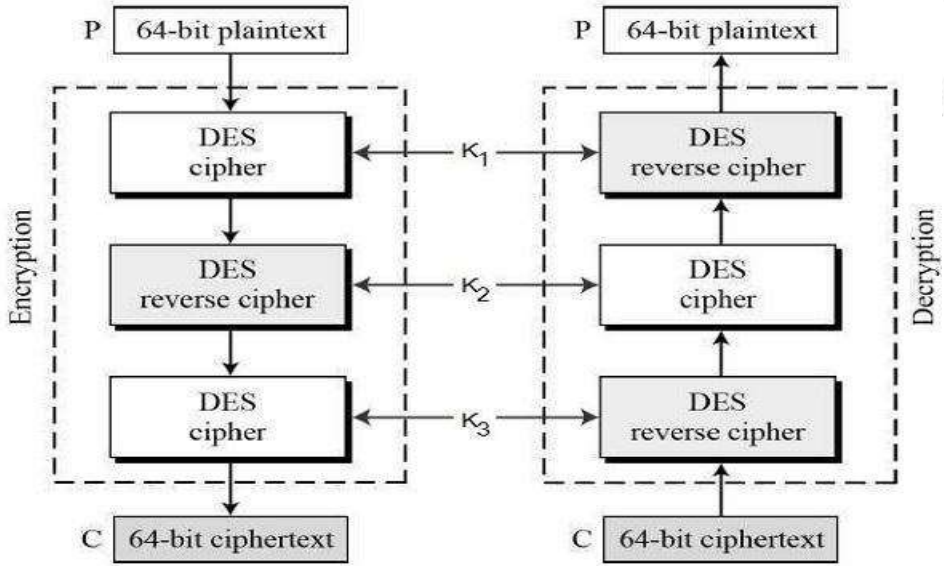
AES algorithm is of three types namely AES-128bit, AES- 192bit, and AES-256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256-bits, respectively. Rijndael method was enhanced to accept extra block sizes and also extra key lengths, but for AES, those functions were not inherited.

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 inter-operation 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.

Rivest Cipher 6 (RC6)

RC6 is a symmetric key block cipher. RC6 (Rivest Cipher 6) is an enhanced version of the old RC5 algorithm. RC6 – w/r/b means that four w-bit-word plaintexts are encrypted with r-rounds by b-bytes keys. It is a proprietary algorithm patented by RSA Security.

RC6 operators as a unit of a w-bit word using five basic operations such as an addition, a subtraction, a bit-wise exclusive-or, a multiplication, and a data-dependent shifting. The RC6 algorithm has a block size of 128 bits and also works with key sizes of 128-bit, 192-bit, and 256 bits and up to 2040 bits. The New features of RC6 include the use of four working registers instead of two and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication significantly increases the diffusion per round, which allow more security, fewer laps and greater performance. Furthermore, like RC5, it can also support various word-lengths, key sizes and number of rounds. RC6 algorithm is very similar in structure to the RC5 algorithm. In fact, RC6 could be considered as two parallel RC5 encryption processes, although RC6 uses an additional multiplication operation that is not used in RC5 algorithm to make the rotation of each bit in a word dependent, not just the least significant bits.

Blowfish

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.

Hybrid Cryptosystem Phases-

The hybrid cryptosystem used to maintain security of the files has two phases:
1. Encryption Phase
2 . Decryption Phase

1. Encryption Phase
At the encryption end,

- On the specification of user, the file being encrypted will be sliced into n slices. Each of the file slices is encrypted using Blowfish key provided by the user for each slice.
- The key will be encrypted using RSA public key
- After encryption, we have encrypted files slices and the corresponding encrypted keys.

2. Decryption Phase
At the decryption end,

- The user will provide n RSA private keys, according to the number of slices (n) created during the encryption phase. Blowfish key is decrypted at the server end using the RSA private key specific to the slice.
- Using the corresponding decrypted Blowfish keys, file slices stored at server are decrypted.
- The decrypted slices will be merged to generate original file.

Design and Implementation

The many advantages of using cloud storage include:

1. It eliminates the need for carrying physical storage devices.

2. Data in any format can be stored using cloud storage.

3. Cloud storage provides safe backup, as opposed to physical storage devices where loss of device, data corruption by a computer virus, natural disasters, amongst other causes, can lead to loss of data.

4. Cloud storage is more cost-effective as it eliminates the need to invest in hardware.

5. Cloud storage also helps developers collaborate and share their work in a more efficient and speedy manner.

Another advantage of cloud storage could be additional security. The proposed system aims to make the cloud storage system secure using data encryption. Thus, the aim of the proposed system is to increase security of data uploaded onto the cloud by using encryption algorithms to make the system more secure.

The system is designed such that it works in the following way:

1. The user signs in if already registered, or signs up to register themselves by providing their details such as name, email id, phone number, password for account etc.

2. The user then selects the file that is to be uploaded by browsing from local storage.

3. The user then selects the encryption algorithm that they want to use. The proposed system provides the choice between using a combination of AES and RSA or AES and Blowfish.

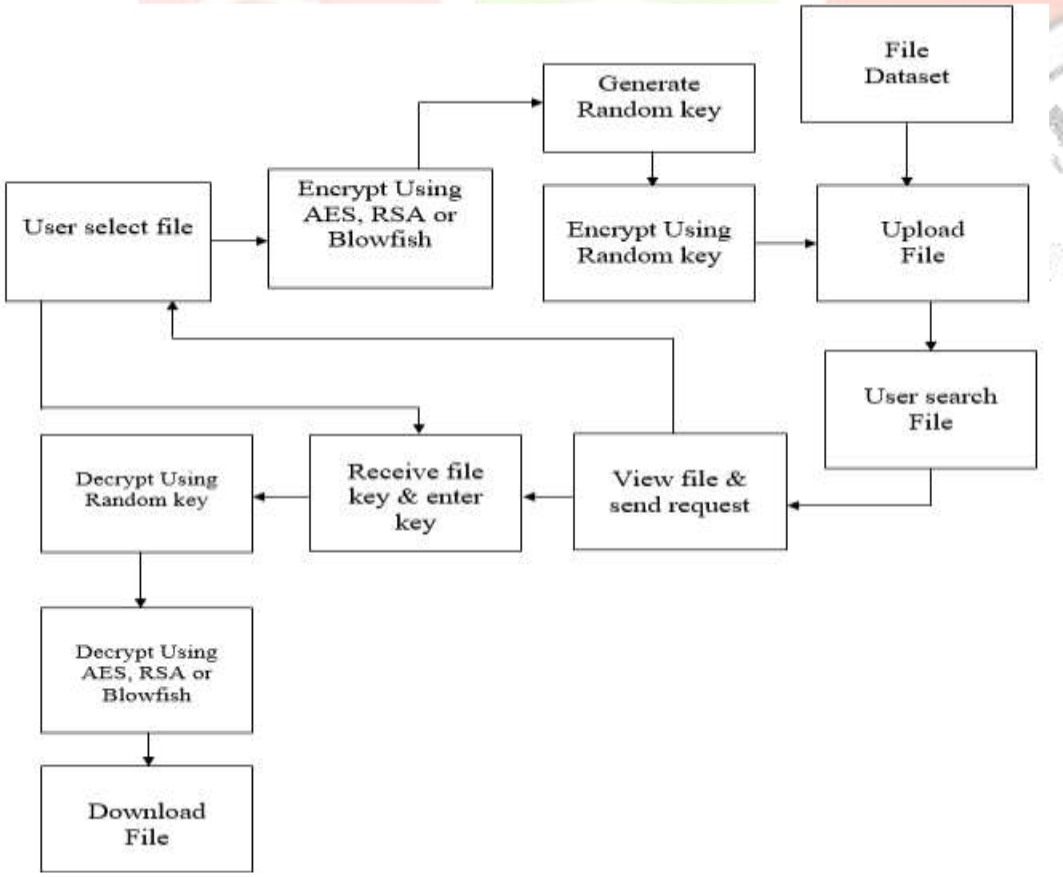
4. The selected file gets uploaded after getting encrypted using the selected encryption algorithm combination.

5. The user also has the option of viewing the files that they have uploaded or have access to and downloading them.

6. On selecting a file to download it, the user is sent the decryption key on their email id that was entered on registration or sign-up.

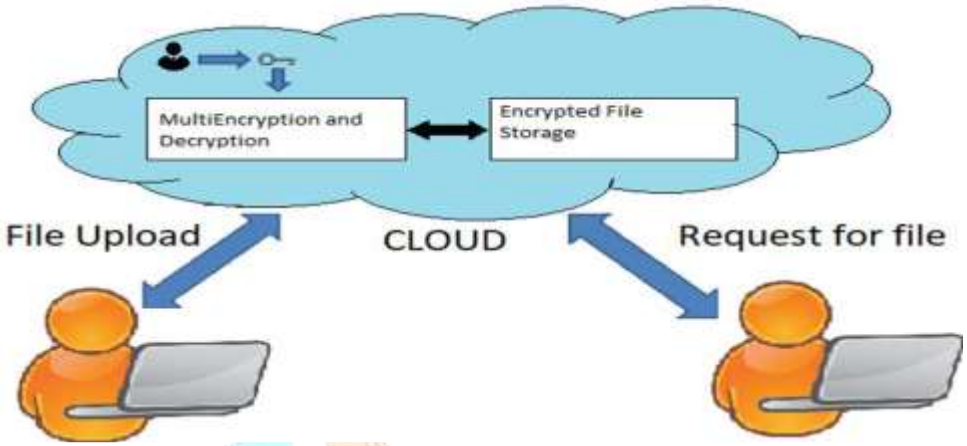
7. Using this key, the user can download the decrypted or original file.

8. The system also provides a comparison with respect to security between the two hybrid encryption algorithm combinations i.e. AES and RSA hybrid combination and AES and Blowfish combination.



Proposed System

In the proposed system, a method for securely storing files in the cloud using a hybrid cryptography algorithm is presented. In this system, the user can store the file safely in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files.



As in the above figure, the files that the user will upload on the cloud will be encrypted with a user-specific key and store safely on the cloud.

1.**User Registration**

For accessing the services the user must first register yourselves. During the registration process various data like Name , username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

2. **Uploading a File on Cloud**

- When the user uploads a file on the cloud first it will be uploaded in a temporary folder.
- Then user's file will be split into N parts.
- These all parts of file will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.
- These all parts of file will be encrypted using different algorithms that are AES, 3DES, RC6. The key to these algorithms will be retrieved from the steganographic image created during the registration.
- After the split encryption, the file reassembled and stored in the user`s specific folder. The original file is removed from the temporary folder.
- Then Combining all Encrypted Parts of file.

3. **Download a File from the Cloud**

- When the user requests a file to be downloaded first the file is split into N parts.
- Then these parts of file will be decrypted using the same algorithms with which they were encrypted. The key to the algorithms for the decryption process will be retrieved from the steganographic image created during the registration.
- Then these parts will be re-combined to form a fully decrypted file.
- Then file will be sent to the user for download.

Conclusion

The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Data security is achieved using RC6, 3DES and AES algorithm. Key information is safely stored using LSB technique (Steganography). Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality. In the future we can add public key cryptography to avoid any attacks during the transmission of the data from the client to the server.

References

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).

Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.

Sunita Sharma ,Amit Chugh:'Suvey Paper on Cloud Storage Security'.

Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).