SECURE FILE SHARING IN CLOUD USING HYBRID CRYPTOGRAPHY

K. Shirisha, Ekta Lahoti , K. Harsha raj, B. Umarani ,Dr.R.Jegedeesan
JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE
KARIMNAGAR, 505 481, TELANGANA

ABSTRACT

Data security is the main concern in different type of applications from data storing in clouds to sending messages using chat. In order to provide security for data in cloud there are many types of techniques which are already proposed like AES, DES, RSA but in existing methods most of the time only single type of encryption was used either AES, OR DES, OR RSA based on user requirement but in this system main problem is each encryption is done using encryption keys if these keys are exposed in any case entire data is lost so we need effective method which can provide more security so in this project hybrid cryptography is used where existing encryption methods are used but three methods will be used. When user uploads data will split in to three parts and first part will be encrypted using AES , second part will be encrypted using DES, third part will be encrypted using RSA and these three encrypted files will be stored in cloud and keys used for AES, DES and RSA are stored in image using LSB steganography when use want to download total data from cloud first keys should be retrieved from image and these keys are used for decrypting data again by using AES, DES and RSA and final data is combined and stored in file. This method provides more security for data

Keywords—Cloud Computing; Decryption; Encryption; Hybrid

1. INTRODUCTION

Today's technologies are growing at very fast speed and deliver the user with many attractive services to reduce the burden of large volumetric data storage and maintenance. Nowadays, many online services are applicable which provides all services and data online such as e-messaging, e-billing, e-transaction, e-mail etc. All these services required user's data online for processing. This data may be any confidential information, which is required by user to be safe from any malicious activity like-healthcare information, bank transaction, credit card details, etc. A high requirement arises for security and protection of data from any unauthorized user as leakage of confidential information may result in serious impairment to user. This increases the security requirement of confidential data before actually migrating it over online internet access. We need to develop a sound, safe and secure framework to protect our confidential data from any such malicious attack. There is a need to convert confidential data into some another form, which becomes inexplicable for any attacker and only authorized users are able to understand that exactly what data is communicated. One of the major techniques to achieve this requirement is cryptography.

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

To maintain security requirements such as data confidentiality and its integrity, authentication is a prime concern to prevent any unauthorized user from sniffing the data to be communicated between two or more parties. To overcome this issue owner needs to first encrypt it before actually transferring it over cloud service provider and provide only authorized users with decryption key. Introduction of cryptography mechanism protects the user data and ensures that the confidential information of user is protected and secure from any unauthorized user access and malicious attack. Unauthorized user tries to hamperthe user's data by altering or modifying it. But due to lack of key it become a tedious task for attacker. Only authorized user has the authority and capability to revert back the converted received data into original form.

2. LITERATURE REVIEW

Many organizations are using cloud computing nowadays like Amazon, Microsoft, Google, and Twitter etc. Cloud computing provides scalable, efficient and pay-per-use services to their user. Cloud computing also provides a lot of features which attracts many researchers to work under different consideration and develop new optimize algorithm related to data security, load balancing, virtualization, concurrency control, resource management etc. A lot of research has been and in-progress in these areas to improve and further introduce new procedure to deliver a comprehensive model.

Prakash et al [1] proposed key relation technique while performing encryption/decryption of file and address the security challenges needs to be resolve in cloud computing. By experiment analysis they had also proved that CA inverter and shifter during encryption and decryption respectively [2] helps to reduce the time complexity as well as deal with various security attacks more efficiently. Fadhil et al [3] proposed a hybrid cryptographic technique by a combination of public RSA cryptosystem and knapsack. This proposed technique is less complex and more secure than individual algorithm. It works in two stages- first perform the RSA encryption and forward its output to knapsack approach. Reverse process needs to be applied while performing the decryption at receiver end. Zissis et al [4] proposed various security issues need to consider while adopting cloud computing such as data integrity, confidentiality, availability, threats, identification and authentication, etc. A new actor namely third-party auditor has also been introducing who will perform auditing on the user request. This auditing feature helps the user to get information regarding its data integrity. Amit et al [5] introduce randomized cryptographic technique. They have introduced the different variations for Ceaser cipher using public key cryptography and randomized technique. Cryptographic techniques utilize the same data. Somdip Dey et al [6] proposed a

new cryptographic technique SDAREE, modified Ceaser cipher bit manipulation technique. It proceeds by removing the redundant text from plaintext to make it more complex and impossible for intruder to break it and get the exact original data. Key will be used in the form of string and generate 'code' and 'power-ex' to be used while performing the encryption. Singh et al [7] proposed a hybrid technique for cryptographic operation which is a combination of Ceaser cipher and Rail fence technique. This integration of transposition and substitution technique provides more secure and efficient approach which is hard to be breach by any intruder.

3. PROPOSED METHODOLOGY

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.

Advantages:

- The key is also safe as it embeds the key using their methods
- The system is very secure and robust in nature.
- Data is kept secured on cloud server which avoids unauthorized access.

4. IMPLEMENTATION

Cloud is playing important role in data management and other type of service which provides secured way of data handling and remote data accessing where users from anywhere can use cloud for data access. As cloud is third party applications where data uploaded by users must provide security features to reduce risks from data attacks in order to do that encryption techniques here used like AES, DES and RSA.

When user uploads data will split in to three parts and first part will be encrypted using AES, second part will be encrypted using DES, third part will be encrypted using RSA and these three encrypted files will be stored in cloud and keys used for AES, DES and RSA are stored in image using LSB steganography.

In the proposed model there are two entities involved which are as follows-

Owner:

Owner will register into the application by providing all the necessary details and therefore he can login into the application using username and password and user can upload the files to cloud and share with the other registered users. He can also view the files uploaded by him and can also view the requests for secret key from the other users and we can respond and the key will be sent to user by mail. Using that key, he can download the file and view the information.

User:

User will register with application and get user name and password. Owner can see all encrypted files uploaded by all users and send request to respective user and get approval to download data and three keys for aes, des, and rsa are shared to owner email which can be used for owner download.

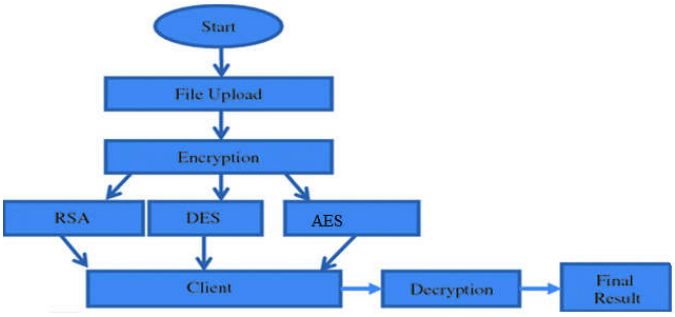
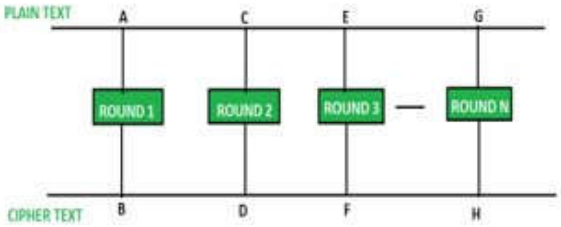


Figure 4.1: Flow Diagram

Algorithms

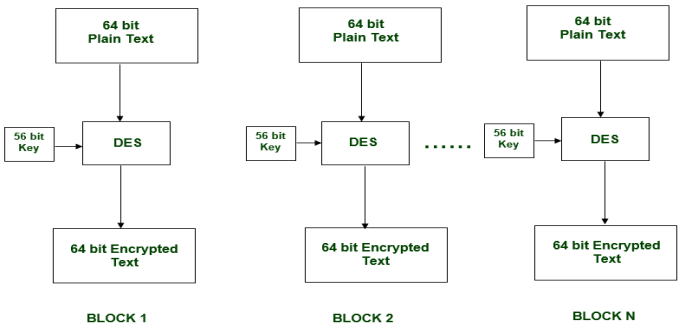
AES (Advanced Encryption Standard)

- It is a majorly used symmetric encryption algorithm better than DES.AES consists of three block ciphers and these ciphers are used to provide encryption of data.
- AES has keys of three lengths which are of 128,192,256 bits. It consists of 10 rounds for 128-bitkeys. Itprovides high security to the users.It requires many rounds for encryption and is hard to implement on software.



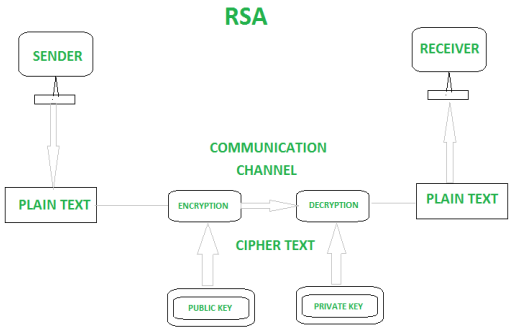
DES(Data Encryption Standard)

- DES is a symmetric cryptographic algorithm encrypts by dividing the data into smaller chunks of 64 bits and then using a 56-bit key with the encryption algorithm to get encrypted 64-bit cipher
- DES uses symmetric key algorithm hence encryption and decryption can be done using single key. DES has fast implementation in hardware when compared to software.



RSA (Rivert,Shamir,Albeman)

- RSA used two keys public key and private key as it is a asymmetric key algorithm.
- A client sends its public key to the server and requests for some data. The server encrypts the data using clients public key and sends the encrypted data. Client receives this data and decrypts it.



LSB (Least Significant Bit)

For each pixel, color is coded with three bytes: red, green and blue respectively. Each byte indicates the intensity of the corresponding color, and the range is from 0 to 255. It takes a byte corresponding to one of the three colors of a pixel, for example 01010110. The idea is to replace these low order bits of information by those that one wishes to conceal. If the message is successfully hidden in well-chosen then image the naked eye cannot perceive the difference.

System Requirements:

Hardware Requirements:

- RAM : 4GB
- System : Laptop
- Processor: Intel core i5

Software Requirements:

- Operating System: Windows 10
- Coding language: Python
- Database: MYSQL

5. RESULT ANALYSIS

The factors included in the algorithm flexibility, suitable for the algorithm process the hardware and software implementation and over all simplicity of process. The before the encryption process the method is divided into the three parts, the encryption using the data using AES for the first portion of data. The DES encrypts the second part and RSA encrypts the third part and finally the data stored in the cloud server.A main specification for the data receivers' needs unique file in downloading the data receiver can transmit the data demand with the authority for the data owner. The access control authority requires the owner. The owners desired in contribution for the original file for the data receiver able to accept the request for processing the data receivers in downloading the data. The downloading process uses the key and mainly valid for the downloading the data with the original format for decryption.

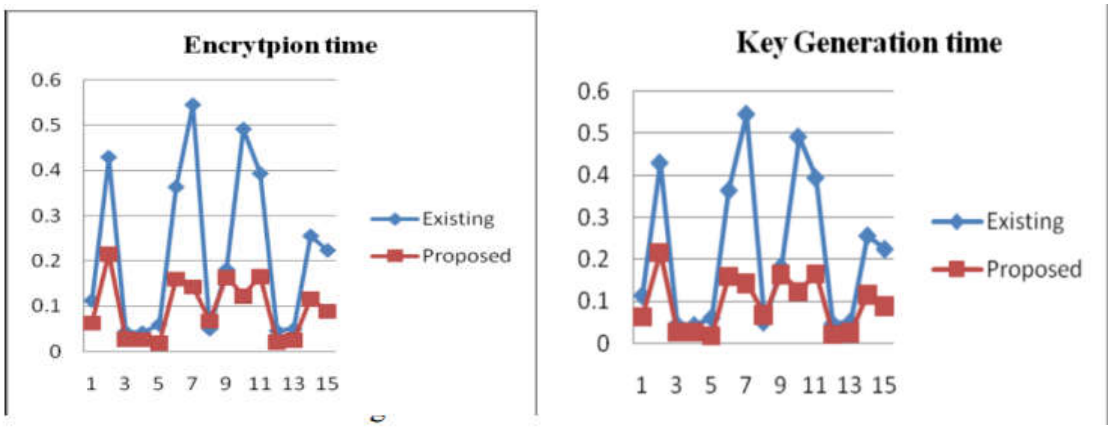


Fig 5.1: A comparison graph for encryption Time and key generation.

6. CONCLUSION

The main goal is to secure store and access data in cloud that is not controlled by the owner of the data. We exploit the technique of AES, DES, RSA cryptography encryption to protect data files in the cloud. Two parts of the cloud server improved the performance during storage and accessing of data. These Encryption algorithms used for encryption is another advantage to improve the performance during encryption and decryption process. We assume that this way of storing and accessing data is much secure and have high performance. Our efforts are going on to solve the problem of security issues by using single encryption algorithm of data in cloud computing environment.

7. FUTURE SCOPE

In proposed system we are using three techniques to encrypt data for security purpose which is shown on cloud environment. As in future scope a multi-dimensional application can be developed where every time when user uploads data user can select what type of

encryption technique, he can use like 2 or three methods based on that each file will have new way of technique.

REFERENCES

[1] G.L.Prakash, M.Prateek and I.Singh, 'Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal of Engineering and Computer Science, Vol. 3, Issue 4, April 2014, pp. 5215-5223

[2]Akshita Bhandari, Ashutosh Gupta, Debasis Das. "A framework for data security and storage in Cloud Computing", 2016 International Conference Techniques in Information and Communication Technologies (ICCTICT), 2016.

[3]Fadhil Salman Abed, "A Proposed Method of Information hiding based on Hybrid Cryptography and Steganography", International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 4, April 2013.

[4]D.Zissis and D.Lekkas, 'Addressing cloud computing security issues', Elsevier Journal of Future Generation Computer Systems, Vol. 28,pp 583-592

[5]Amit joshi and Bhavesh Joshi "A Randomized Approach for Cryptography" International Conference on Emerging Trends in Network and Computer Communications (ETNCC), pp. 293- 296, April 2011.

[6]Somdip Dey "SD-AREE: An Advanced Modified Ceaser Cipher Method to Exclude Repetition from a Message" International Journal of Information & Network Security (IJINS). Vol. 1, Issue. 2, pp. 67-76, June 2012.

[7]Ajit Singh, Aarti Nandal and Swati Malik, "Implementation of Ceaser Cipher with Rail Fence for enhancing data Security", International 978-1-7281-1253-4/19/$31.00 © 2019 IEEE Journal of Advanced research in Computer Science and Software Engineering. Vol 2, Issue 12, pp. 78 -82, December 2012.

[8]Jitendra Singh Adam et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.

[9]Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.D.Baswaraj, J.Greeda 2019 "Improved Migration Performance In Virtualized Cloud Datacenters" International Journal of Scientific & Technology Research. Volume 8, Issue 09,page no.1515-1518 September 2019. (Scopus indexed)

[10].Annadi Jahnavi, Hanumandla Bhavana, Dr. R. Jegadeesan "An Implementation of Detecting Password Pattern In Dictionary Attack" International Journal of Advanced Science and technology. ISSN 2005-42386, Page no: 84-92 July,2019(Indexed by Scopus, Elsevier).

[11].Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.C.N.Ravi, J.Greeda2019 "A Secure Transaction Authentication Scheme using Blockchain based on IOT" International Journal of Scientific & Technology Research. VOLUME 8, ISSUE 10,Page no:2217-2221 OCTOBER 2019. ISSN 2277-8616 (Scopus indexed)

[12].Dr R Jegadeesan, Dr.C.N.Ravi, Dr.A.Nirmal Kumar 2020 "Automatic Rice Quality Detection Using Morphological and Edge Detection Techniques" ICCCE 2020 3rd International Conference on Communications and cyber Physical Engineering, Metadata of the chapter that will be visualized in Springer Link. Volume, issue, May.2020 Page No.233-242, Springer conference.