International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017
Issue 11, Volume 4 (November 2017) www.ijiris.com

HYBRID CRYPTOSYSTEM FOR SECURE DATA STORAGE

Mihir Shah
Information Technology, Mumbai University
mihir.vs@somaiya.edu

Prof. Sujata Pathak
Information Technology, Mumbai University
sujatapathak@somaiya.edu

Manuscript History
Number: **IJIRIS/RS/Vol.04/Issue11/NVIS10080**
DOI: 10.26562/IJIRIS.2017.NVIS10080
Received: 03, October 2017
Final Correction: 12, October 2017
Final Accepted: 24, October 2017
Published: November 2017
Citation: Innovative Research Journal in Information Security, Volume IV, 01-04
doi:10.26562/IJIRIS.2017.NVIS10080
Editor: Dr.A.Arul L.S, Chief Editor, IJIRIS, AM Publications, India

Abstract— Cloud computing has become an integral part of most of the private and public organizations and being used for data storage and retrieval. There are many usage of cloud computing and widely used in highly confidential national services like military and treasury for storing confidential information. The cloud computing for example Google drive, Amazon Web Service and Microsoft Azure are beneficial for organizations and end-users. Using Cloud computing and its services, organisation/end-users can store their data. There are multiple challenges while saving organisations highly confidential documents in servers. Hence, the objective of this paper is to provide a high level design for a storage system maximising security and personal privacy. Though servers are highly protected against unauthorized access, there are incidents where confidential files stored on servers are accessed by the maintenance staffs. Hence this research paper provides introductory structure for fully protection of files stored in the server by using Hybrid Cryptosystem.

Keywords — Cryptography, Encryption, Decryption, Steganography, Security

I. INTRODUCTION

The cloud is popular to store data and files due to the low costs, less maintenance and ease of access from any location. Apart from the private and public organizations, government services are looking for cloud based storage and services for their confidential data storage. Every cloud provider like Microsoft Azure, IBM, Amazon Web Services (AWS) and many others have provided their own technique to encrypt and decrypt the data. The cloud computing is widely used in private and public services organizations for storing huge amount of data which can be made available from any location. The usage of cloud is found in industry, military colleges, and private organizations. The data stored on the cloud is accessible by user authentication but for confidential access multiple layer of security is implemented. The algorithm of this multiple layer security is dependent on the level of privacy. To provide the solution to different levels of security, cryptography and steganography techniques are popular. Multiple algorithms must be incorporated to enhance the level of security in data storage. New technique, using symmetric key cryptography algorithm and steganography is proposed in this work.

While accessing the data on cloud front end interface, business layer and data storage layers are used. Though the front end resides on user computer but the business and data layers reside on service provider premises. Hence the encryption algorithm is implemented by the cloud service provider. The challenge in encryption is that more complex logic slows down the reading and writing of the files on the server and hence the algorithm is applied only when it is needed. Encryption algorithm helps to solve this problem by encrypting the files. This purpose of this research is to present a file security model for the solution of security issue in cloud environment. In this model, hybrid encryption is used where files are encrypted by 6 algorithms coupled with file splitting which is used for the secured communication between users and the servers.

II. LITERATURE REVIEW AND EXISTING SYSTEM

Data Security Issues [5] are main issue in the existing system. Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:

1. 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 a threat or has been compromised.
2. 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.
3. Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

The word cryptography means changing the message data into a scrambled code which can be retrieved back on open network. Cryptography technique secures the sensitive information in unsecured transmission networks and which can be read by intended recipient. A cryptography algorithm needs a key along with a message of any format to form the cipher text. The level of security of cipher text depends on the strength of cryptographic algorithm and privacy of the cryptographic key used. Thus the first level of security has been provided. Further security can be improved using yet another Data hiding technique, Setganography. In this proposed system AES, DES, RC2 algorithms are used to provide block wise security to data. Key information security is implemented by using LSB steganography technique. The purpose of Key information is to decide link between available algorithm and key file encryption. By using this technique the file is fragmented into three parts and each part uses unique algorithm technique. Multithreading is used to encrypt every part of file simultaneously for improving the performance. LSB technique is used to insert Data encryption Keys into cover image. Valid user receives an email with Stego-Image of the key. Reverse process of encryption is applied for file decryption purpose. Symmetric key cryptography algorithms are AES, DES, 3DES, IDEA, BRA, ECB, CBC and blowfish [3]. These algorithms accomplished high level security but increase delay for data encode and decode. Steganography hide the secret data existence into envelope. In this technique existence of data is not visible to all people. Only valid receiver knows about the data existence. Image steganography technique is used to produce high security for data. Secret data of user hide into image file. After adding text into image file it looks like normal image file. DES algorithm is used for text encode and decode. Advantage of image steganography technique is providing security to text.

Three bit LSB technique used for image steganography. We can hide huge amount of into image using LSB steganography technique. AES is symmetric key cryptography algorithm. It supports three types of keys. For 128 bit key require 10 rounds, 192 bit key require 12 rounds and 256 bit key require 14 rounds [6]. In improved AES algorithm encryption and decryption time is reduced .Advantage of modified AES algorithm is provides better performance in terms of delay [1]. DES applies a single key for texts encode and decode. Size of key is 128 bit. In this algorithm many steps are executed randomly so illegitimate user cannot even guess the steps of algorithm. Provide high throughput is one of the advantages of symmetric key cryptography algorithms. [4] Improved DES algorithm uses 112 bit key size for data encode and decode. Key generation process is done using random key generation technique. It provides security to data. Disadvantage of this algorithm is essential maximum time for converting data into cipher text because it operates on single byte at a time.

III. PROPOSED SYSTEM

The solution of the asymmetric cryptography is enhanced with the additional layer of security by combining AES, DES, RC6, ECB, CBC, Triple DES algorithms. The proposed system is a process development for file security issues in storage systems. Same concept as of cloud computing is implemented with new technique and method, where user can store data and can access it using proposed system. The overall proposed system structure is shown as below figure 1.

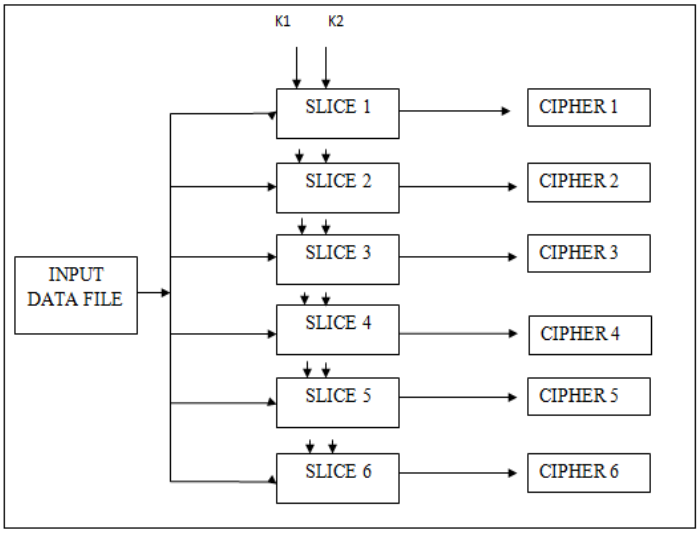

Fig. 1: Proposed Storage Architecture

The encryption of the multimedia files and images are stored using the steganography technique as shown in the figure 2.

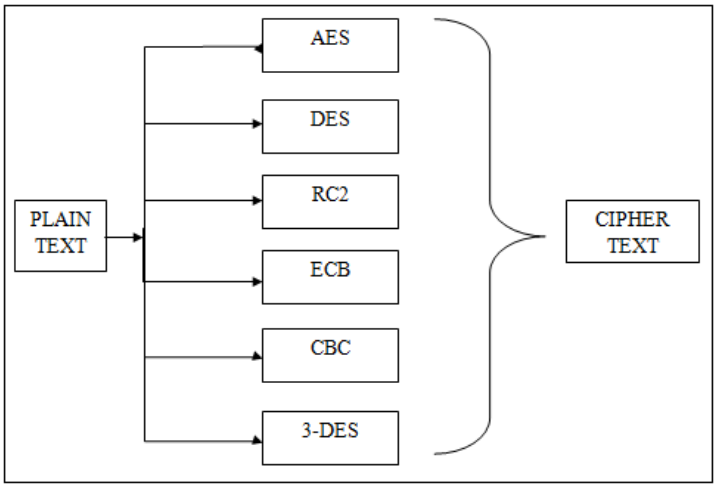

Fig. 2: Encryption Algorithm for each data part.

In this proposed system AES, DES, RC2, ECB, CBC, 3DES algorithms are used to provide block wise security to data. LSB steganography technique is introduced for key information security. Key information contains which part of file is encrypted using by which algorithm and key. File is fragmented into 3-6 parts as per user input. Each and every part of file is encrypted using different algorithm.

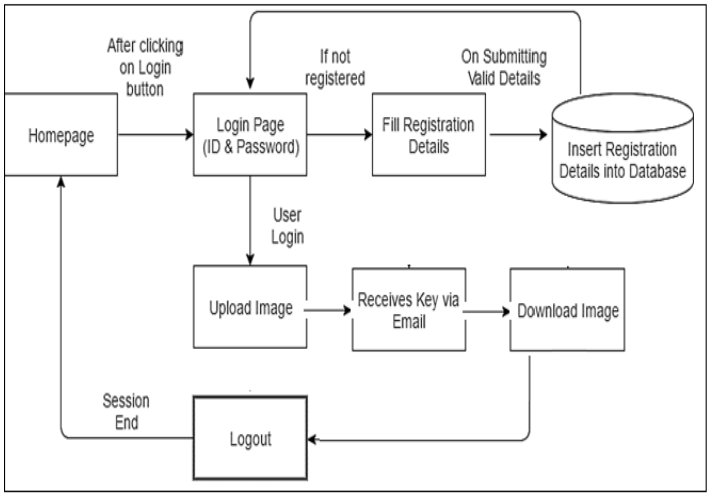

Figure 3: Overall System Architecture

All parts of file are encrypted simultaneously with the help of multithreading technique data encryption Keys are inserted into image which is used as a key, using LSB technique. Stego-Image is send to valid receiver using email. For file decryption purpose reverse process of encryption is applied. Figure 3 provides an overview of system architecture. In order to ensure file security on storage system, the above hybrid cryptosystem is deployed on server/cloud/local system. The scheme deployed is in three phases as listed.

1. Registration Phase
2. Uploading Phase
3. Downloading Phase

The phases of implementation are explained below.

1. Registration Phase:
In the Registration Phase, the end users register in order to upload and view files to/from the storage server.

2. Uploading Phase:
The files are uploaded by the end users to the registered server. The encryption of uploaded files is done using the hybrid cryptosystem. The private keys i.e. stego-image is sent to user over mail so that authenticated user can view uploaded file.

3. Downloading Phase:
On successful authentication, the user provides the private key i.e. stego-image for the corresponding n slices. The private keys decrypt the corresponding encrypted slices. The decrypted files are merged to generate original file. The decrypted file is downloaded and viewed at user end.

IV. CONCLUSIONS

Data Security and Privacy of data stored in have full of challenges. Continuous research is going on to improve the data storage security. This paper presents hybrid security algorithms using the symmetric key. This approach helps in reducing the encode and decode time and hence help in improving the performance for storing large data files in highly secured environment. Because the key is secured, it can only be accessed by the authorized user. The algorithm is built and computed on cloud server so that data movement traffic is minimized. The solution proposed in this research provides additional layer of security by combining AES, DES, RC6, ECB, CBC, Triple DES algorithms to asymmetric cryptography. This technique helps to apply the key information on data storage (server storage system).

ACKNOWLEDGMENT

I am very thankful to my guide Prof. Sujata Pathak for her invaluable guidance and advice throughout this project.

REFERENCES

1. Y Manjula, K B Shivakumar. Enhanced Secure Image Steganography using Double Encryption Algorithms, at International Conference on Computing for Sustainable Global Development IEEE, 2016.
2. Aarti Singh, Manisha Malhotra. Hybrid Two-Tier Framework for Improved Security in Cloud Environment, at International Conference on Computing for Sustainable Global Development IEEE, 2016.
3. Vishwanath Mahalle, Aniket Shahade. Enhancing the data security in cloud by implementing Hybrid (RSA & AES) Encryption Algorithm, International journal of pure & applied research in engineering and technology, 2016.
4. Sakinah Ali Pitchay, Wail Abdo Ali Alhiagem, Farida Ridzuan, Madihah Mohd Saudi. A proposed system concept on Enhancing the Encryption and Decryption Method for Cloud Computing, 17th UKSIM-SMSS International Conference on Modelling and Simulation, 2015.
5. K.Yang, J.Xiaohua. Security for Cloud storage systems, Springer Brief in Computer Science, 2014.
6. C.K Chan, L.M Cheng. Hiding data in images by simple LSB substitution, Pattern Recognition, vol.37, pp. 469-474, 2014.
7. M.S Sutaone,M.V Khandare. Image based Steganography using LSB insertion Technique, IET International Conference, 2008.
8. Prof. Vishwanath S. Mahalle. Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing, International journal of pure & applied research in engineering and technology, 2013, volume 1(8):220-227, ISSN-2319-507X IJPRET.

