DOI: http://dx.doi.org/10.26483/ijarcs.v9i3.5749

ISSN No. 0976-5697

Volume 9, No. 3, May-June 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ENHANCING ALGORITHMS FOR SECURED DATA STORAGE IN PUBLIC CLOUD ENVIRONMENT

Prof.Prabu.S
Senior professor
Department of computer science, VIT University
Vellore, India

M.Manideep
Student
Computer Science, VIT University
Vellore, India

Abstract: Now a day's cloud computing is used in many areas such as industry, military, colleges etc to store huge amount of data. We can retrieve data from cloud on request of user. To store data on cloud we have to face many issues. To provide the solution to these issues there are n number of ways. Cryptography and steganography techniques are used now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. In my project I have introduced new security mechanism using symmetric key cryptography algorithm and steganography. In this proposed system AES, DES, and RC6 algorithms are used to provide block wise security to data. All algorithm key, size is 128 bit. LSB steganography technique is introduced for key information security. Key information contains part of file is encrypted using by which algorithm and key. File is splited into three parts. Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption Keys are inserted into cover image using LSB technique. Stego image is send to valid receiver using email. For file decryption purpose reverse process of encryption is applied.

Keywords: Cryptography, cloud computing, multithreading, Advance Encryption Standard, Data Encryption Standard

I. INTRODUCTION

Our paper introduces a new model for file security which provides an efficient solution for storing the file in the cloud environment. This model is known as Hybrid Cryptosystem model where we add double -layer security to store the file in the cloud environment. This paper presents cryptography and steganography techniques. In the cryptography technique, we use hybrid encryption where each file is split into three equal parts in which each part of the file is encrypted using 3 encryption algorithms which are AES, DES AND RC6 and we use image steganography method using LSB technique. AES algorithm has been embraced by the U.S. government and presently utilized around the world. It replaces the Data Encryption Standard (DES) algorithm which was announced in 1977. AES is a symmetric key algorithm where a similar key is used for encryption and decryption. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effectivekey length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).[1]

In cryptography, RC6 (Rivest cipher 6) is a symmetric key block cipher derived from RC5.RC6 generally has a block size of 128 bits and key sizes of 128, 192, and 256 bits, but, like RC5, it may be parameterized to help a wide assortment of word-lengths, key sizes, and the number of rounds.RC6 is fundamentally the same as RC5 in structure, using data-dependent rotations, and XOR activities; in fact RC6 could be seen as entwining two parallel RC5 encryption forms, in spite of the fact that RC6 uses an additional increase task not present in RC5 so as to make the turn subject to each piece in a word, and not just the least significant few bits.[1]

The Objective of this proposed model is to provide Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption Keys are inserted into cover image using LSB technique. Steganography image is send to valid receiver using email. For file decryption purpose reverse process of encryption is applied. [1]

The proposed hybrid model is likely to meet the security needs of Data in the cloud. The hybrid encryption technique which uses 3 encryption algorithms take minimum time and maximum throughput for both encryption and decryption part compared to other symmetric algorithms. The idea of splitting and merging the file is likely to meet the data security principle. The hybrid model, when replenished in the cloud the remote server more secure and along these lines, causes the cloud suppliers to get more trust of their clients. For information security and protection assurance issues, the basic test of a partition of sensitive information and access control is satisfied. [2]

II. OVERVIEW OF PROPOSED MODEL

To ensure the security of a file in the cloud our proposed hybrid crypto model has to be deployed in the cloud. We expect cloud server as trusted however with a specific end goal to avoid misuse of data by an intruder or data leakage or other security problems, the data is stored on the server in the cipher text. We generally classify the model deployed on the cloud in three stages: [2]

A. REGISTRATION PHASE

In the Registration Phase, the client registers himself in order to upload and view his files to/from the cloud server.

B. UPLOADING PHASE

The files are uploaded by the user to the server. The encryption of file is done by hybrid encryption technique. The image file is encrypted by steganography technique. The security key is send to the user so that only the Authenticated user is able to his uploaded or download file.[3]

C. DOWNLOADING PHASE

On successful authentication, the client will input the private key for the corresponding n slices. The private keys will decrypt the corresponding encrypted image. The decrypted files are merged togenerate original file. Thedecrypted file is downloaded and viewed at client end. [3]

III. MODULES AND REQUIREMENT ANALYSIS OF HYBRID CRYPTO SYSTEM

The system comprises of 4 modules as follows:

A. REGISTER/LOGIN

User need to register first by filling up basic registration details. Using the login id and password, user can login into the system. [4]

B. UPLOAD IMAGE

Here, the image file to be stored is encrypted using **AES** (Advance Encryption Standard), **DES** (Data Encryption Standard) and **RC6** (Rivest Cipher 6) encryption algorithm.**LSB** (Least Significant Bit) steganography technique is introduced for key information security**.** Key information contains which part of file is encrypted using which algorithm and key. [4]

C. SEND MESSAGE VIA MAIL

This encrypted file is sent along with the image containing the key that is hidden in the image using LSB. [4]

D. DOWNLOAD IMAGE

Here, when the user request for a file to be downloaded, then that file is decrypted using AES, DES and RC6.After successful decryption, the image file is merged into one file and then downloaded. The key is extracted from the image**.**After the file is downloaded. [4]

The Requirement Analysis as follows

E. PRODUCT PERSPECTIVE

The product will help the user to secure the file in cloud by three encryption algorithms in a secure mannerand file stored in the cloud can only be accessed by shared or authenticated user. [5]

F. PRODUCT FEATURES

The product uses 3 encryption algorithms to secure the file in cloud and product also uses steganography technique

G. CLIENT CHARACTERISTICS

Client should check and upload the picture has sent to authenticated user only. Client should give a Security key to embed it into picture which is an image steganography technique

H. ASSUMPTIONS AND DEPENDENCIES

The results highly depends on the sever connection and its response of sending the encryption image to the user's email and merge the security key with in the picture. So we should check any errors and correct them. [5]

I. DOMAIN REQUIREMENTS

There should be visual studio software provided in the system. The Data bases and server should be integrate correctly to validate login using my sql server

J. USER REQUIREMENTS

User details has to be registered in database if not user has to register their details through register page or phase. User should provide his e-mail correctly and check for the encrypted image from client to access the file. [5]

IV. ARCHITECTURE

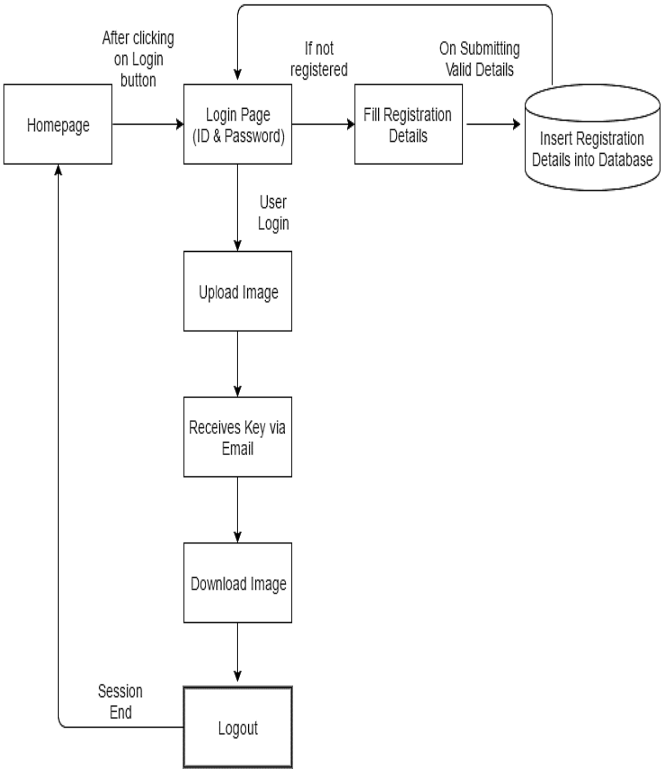
After clicking on Login button
If not registered
On Submitting Valid Details
Homepage
Login Page (ID & Password)
Fill Registration Details
Insert Registration Details into Database
User Login
Upload Image
Receives Key via Email
Download Image
Session End
Logout

Figure 1: SYSTEM ARCHITECTURE

V. RESULTS AND DISCUSSION

A. SAMPLE TEST CASES

User Login/Registration: To begin with login, user need to register by filling up basic registration details. There are multiple fields in registration page and every field has to fill by user. User cannot use character in the login id field. [6]

VALIDATION CRITERIA

- In each form, no field which is not null able should be left blank
- All numeric fields should be checked for non-numeric values. Similarly, text fields like names should not contain any numeric characters.[6]
- All primary keys should be automatically generated to prevent the user from entering any existing key.[7]
- Whenever the user Tabs out or Enter from a text box, the data should be validated and if it is invalid, focus should again be sent to the text box with proper message.[7]

B. ADVANTAGES

- The stored image file is completely secured, as the file is being encrypted not by just using one but three encryption algorithm which are AES, DES and RC6.[8]
- The key is also safe as it embeds the key in image using LSB.[8]
- **Performance and Availability**: -There is one other issue of cloud data storage that after storing our data in cloud data storage we have very comfortable for access our data in any place or in any location without carrying data to everywhere.[9]
- **Privacy**:-In cloud computing data storage system all users know that Different from the traditional computing model, utilizes the virtual computing technology. Its mean User's personal data may be distributed in various virtual data center rather than stay in the same physical location. At this time, data privacy protection will face the controversy of different legal systems.[9]

C. APPLICATIONS

This application is useful for storing an image file that contains very sensitive information. For example, any company important file.

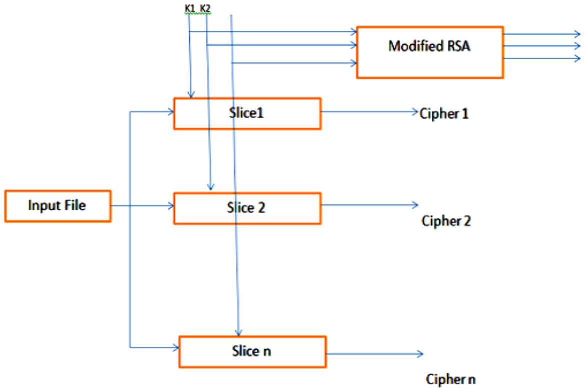

Figure 2: file encrypted by hybrid approach

VI. CONCLUSION

Data Security and Privacy of cloud data stored in Cloud Computing has full of challenges and of. Many research problems are yet to be come which are increase the security problem the cloud data storage's this paper present hybrid security algorithms using the symmetric key. The only difficult task is here that the key is secure. That are only accessible by the authorize user. And the purpose of using that key is to save more time to store the large amount of data in cloud date storage. And the purpose of these algorithm is generally in cloud data storage (server storage system) not in travelling the data between the users by secure channel.

VII.REFERENCES

[1]. Punam V. Maitri, ArunaVerma." SecureFile Storage in Cloud Computing using hybrid Cryptography Algorithm". IEEE INSPEC pp. 23-25 Mar. 2016

[2]. Shweta Kaushik, Charu Gandhi, "Cloud Data Security with Hybrid Symmetric encryption". IEEE INSPEC pp. 11-13 Mar. 2016

[3]. S. Hesham, Klaus Hofmann, "High Throughput Architecture for the Advanced Encryption Standard Algorithm", IEEE International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pp. 167-170, April 2014.

[4]. Yingbing Zhou, Yongzhen LI, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", IEEE ICSESS, pp. 517-520, June 2014.

[5]. K. Jasleen, S. Garg, "Security in Cloud Computing using Hybrid of Algorithms", IJERJS, vol. 3, no. 5, pp. 300-305, September–October 2015, ISSN 2091-2730.

[6]. R Kiruthika, R Jeena, "Enhancing Cloud Computing Security using AES Algorithm", IJARCSSE, vol. 5, no. 3, pp. 630-635, March 2015, ISSN 2277 128X.

[7]. SomdipDey "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, June 2012, pp. 67-76

[8]. Sinkov A., "Elementary Cryptanalysis – A MathematicalApproach", Mathematical Association of America, 1996

[9]. S. Munjall, S. Garg, "Enhancing Data Security and Storage in Cloud Computing Environment", IJCSIT, vol. 6, pp. 2623-2626, 2015, ISSN 0975-9646.