Secure Storage Service on Cloud using Hybrid Cryptography Approach.

Aniruddha Gandhare, Rupesh Mali, Sanket Sahane, Dhananjay Deshmukh, Abhinay G. Dhamankar
Information Technology Department, Pune Institute of Computer Technology, Pune, Maharashtra, India
anirudhag1999@gmail.com, rupeshmali670@gmail.com, sanketusahane@gmail.com,
deshmukhdhananjay06@gmail.com, agdhamankar@pict.edu

***Abstract*—Security of data has been the biggest concern in the past couple of years. The existing systems are not quite helpful in securing the sensitive data of the users. It has been difficult to secure and manage data that has been uploaded to the cloud. The encryption that is used in existing systems is not enough and can be the biggest flaw in security scams. To overcome this flaw or problem the proposed system will be using a hybrid cryptography approach. The system will be using multiple encryption algorithms to encrypt the data that will be stored on the cloud or uploaded to the cloud. When the user will upload the file to the cloud, the server will get the file and split it into three files. Each file will be then sent to particular encryption algorithms. The three encryption algorithms that the system will be using are AES256, RC4, Blowfish. These 3 algorithms are good and efficient for this type of system. The first file part will be provided as input to the AES256 algorithm, the second file will be provided as input to the RC4 algorithm and the last file will be provided to the blowfish algorithm. All the files will be then uploaded to the different Aws s3 buckets. The keys that will be generated will be embedded into respective images and stored into image storage services. This will provide more security to the user data. During the download process the whole procedure will be reversed. When the user requests for the file, the server will refer to the metadata and request the file from the cloud. The encrypted file will be split into 3 parts and each file will be provided as input to the respective algorithm. The files will be decrypted using the respective algorithm and then merged to a single original file that will be sent to the user as response. The whole process will take more time so to tackle this,the system will be using node js for performing asynchronous calls and functioning.**

Keywords— encryption, hybrid cryptography, AES, RC4, Blowfish. cloud.

I. Introduction

Cryptography is a way of encrypting data into its safest form which helps maintain data integrity and consistency. There are 2 types of encryptions namely symmetric key encryption technique and asymmetric key encryption algorithm. These techniques use a key to encrypt data and store it in the safest way possible. The symmetric key encryption algorithms are AES, DES, Blowfish and 3DES. RSA is an example of asymmetric encryption. The AES 256 algorithm is one of the safest algorithms present and has had a great impact on the information security field. These encryption algorithms are used to encode and decode data. There are other cryptography techniques such as Steganography, where a message is hidden in an image using various techniques. The steganography technique is effective as only a valid receiver knows that a message is hidden in an image.

II. Related Work

Hybrid cryptography algorithm presented by author A. Shahade. AES and RSA are used in hybrid algorithms. AES algorithm uses a single encryption key. In the hybrid encryption algorithm there are three keys. Data has been uploaded to the cloud so the mandatory keys are AES secret key and RSA public key. The RSA secret key and AES secret key is important to download data from the cloud. Whenever a user makes an attempt to download a file from the cloud that file is stored into the directory for a short time. During the encryption process first AES is applied on the file and then RSA algorithm is applied on the encrypted data. The reverse process is used to decrypt data. After the encryption that file is stored on the cloud. By using hybrid cryptography there are many advantages like data integrity, security, confidentiality and availability. The RSA algorithm does take too much time to encode the data [1]

A hybrid algorithm consists of three algorithms. For user authentication digital signatures are used. For better confidentiality, a blowfish algorithm is used. The blowfish algorithm uses a single key and needs the least amount of time for encode and decode. The concept called sub array key is used in the blowfish algorithm. The main purpose behind this hybrid cryptography algorithm is to achieve high level security for data that is being uploaded to the cloud. [2]

III. Methodology

All these above approaches have their ups and downs. As the single encryption algorithm is not that reliable so using a hybrid approach for encrypting cloud data is a must. The Hybrid cryptography approach ensures high data security. Using Blowfish with AES and RC4 algorithms is an optimal solution and can be used to decrease the time taken to complete the encryption process.

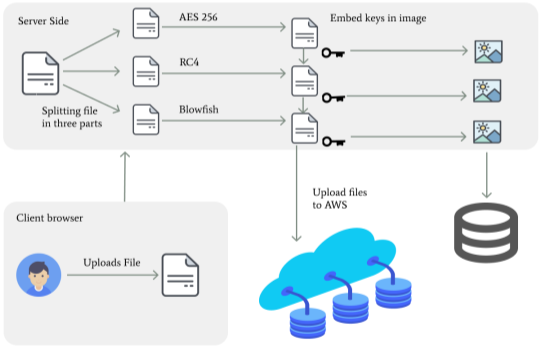

Fig 1.1- Architecture diagram

User file upload Module:

1. In this module the user can log in to the system and view files and folders.
2. The user can also upload files from his local storage and will get a response once it is uploaded.

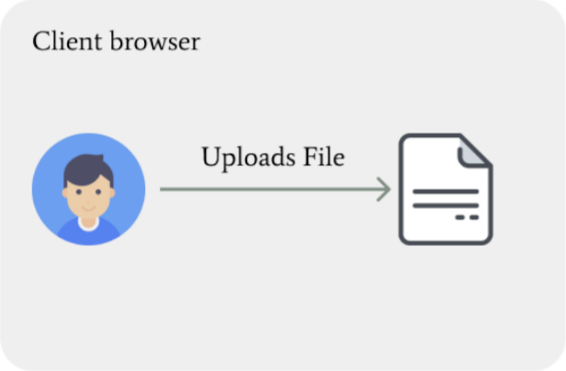

Fig 1.2- File upload module

Splitting Module

1. The file that will be uploaded by the user will be splitted using a splitting algorithm in three parts. This file will then be sent to the encryption module.

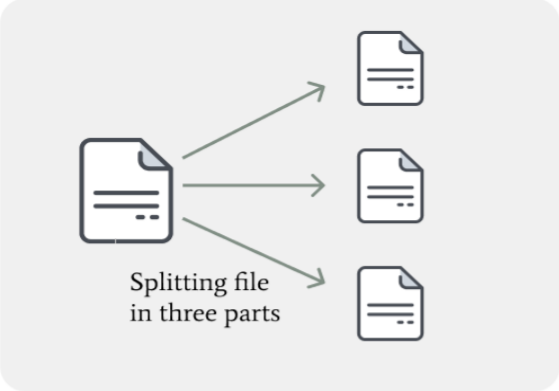

Fig 1.3- File splitting module

Encryption Module

1. This module will take the three splitted files as input for encryption.
2. The first file will be provided as input to the AES algorithm, the second file will be given as an input to the RC4 algorithm and the third file will be given as input to the Blowfish algorithm.
3. A key will be generated during the encryption process.
4. These files will be uploaded individually to different locations on the cloud.
5. The keys that were generated during encryption were .
6. Now the final encrypted file is ready for uploading on the cloud.

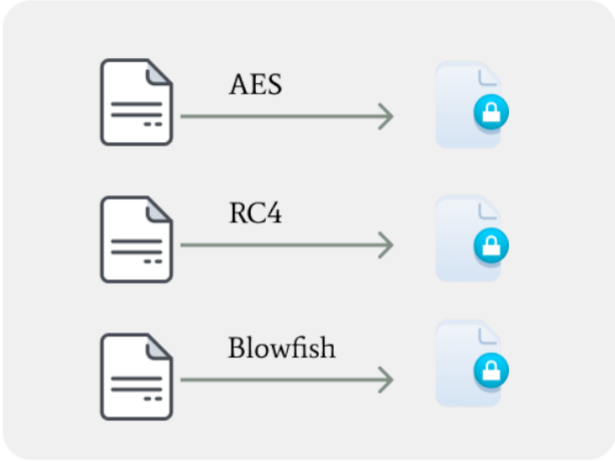

Fig 1.4 - File Encryption module

Steganography Module:

1. Now in this module the keys will get embedded in the respective images using steganography.

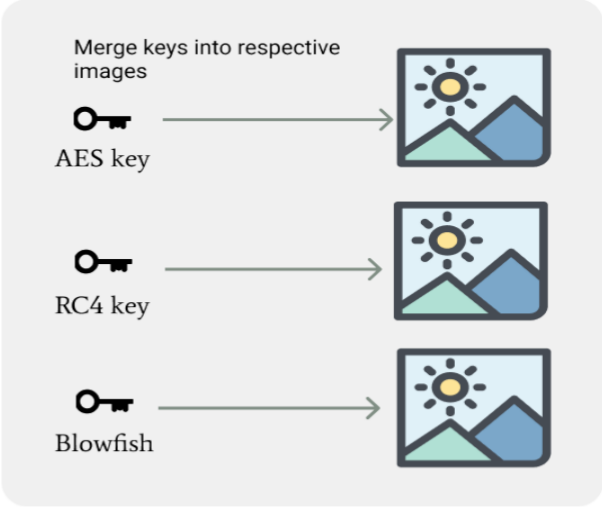

Fig 1.5- Steganography module

Files upload to AWS S3 Module:

1. When the files are encrypted they will be stored on AWS cloud on different locations.

IV. RESULT ANALYSIS

The proposed system uses AES, RC4 and Blowfish for better security and encryption standards. The Proposed system is the hybridization of AES, RC4, Blowfish which are fast and secure. These algorithms are symmetric key algorithms. The AES uses a 256 bit key for encryption and RC4 also uses a 256 bit key and blowfish is a variable key cryptography technique. To hide keys in image for better security practices LSB technique of steganography is used which will hide the keys in a cover image. The file encrypting and decrypting speeds are analysed using java. The time is only calculated for text files with comparison of existing AES and Blowfish algorithm encoding algorithms.

The file encoding and decoding time is being tested individually and on each file. The speed of the whole process is decreased by using node js. Node js is an asynchronous language and supports Non blocking IO. The advantages of using node js is that the system doesn't wait for IO operations to get completed instead it executes further code which gives faster execution time. The files will be splitted using a splitting algorithm which will use modulus for dividing the files. The original file size will be divided by 3 and the first two files will be of the same size. The third file will be of size (size of first file) + (File size % 3). When the files are checked for errors and if there are no errors each file will be given as an input to an encryption algorithm.

Once the file is sent to encryption the user gets a success message and file metadata is stored in mongo db database. The files will get encrypted and stored in an AWS S3 bucket. Each file will be stored in a different bucket and the information about this will be stored in metadata of that particular file. The keys will be generated during the encryption algorithm and will be embedded into an image using steganography. The steganography image will be stored to an image storage service.

One of the main concerns in this project was speed of the algorithms. All the three algorithms are quite fast and secure and reliable when used together. Following are speed comparisons AES and Blowfish encryption speeds.

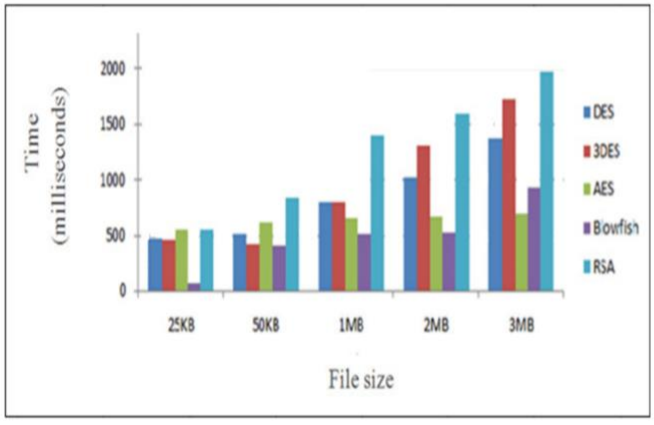

Fig 1.6- Comparison of encryption time

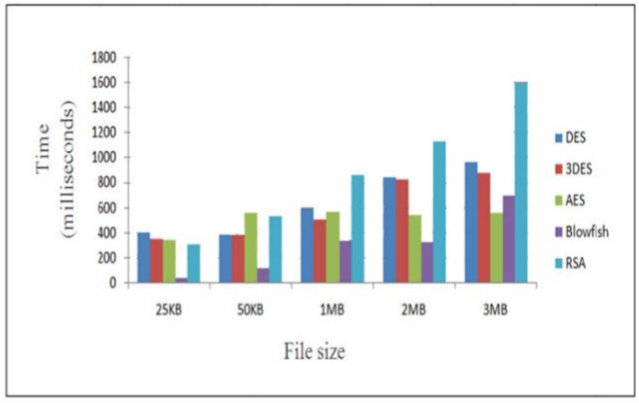

Fig 1.7- Comparison of decryption time

V. CONCLUSION

Cloud storage issues are solved using hybrid cryptography approach. All encryption techniques use a block wise data encryption except RC4 which is a stream cipher. Key security is achieved by LSB technique of steganography which hides the key in a cover image. The delay parameter is reduced by making use of multithreading technique and with help of node js non blocking io. The various algorithms used in the proposed system will ensure data integrity and confidentiality. The time required to encrypt and decrypt is quite less than the existing systems that use AES and Blowfish. Thus providing a fast and secure way of securing data over cloud.

REFERENCES

[1] V.S. Mahalle , A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE , INPAC,pp 146-149,Oct .2014

[2] Jasleen K., S.Garg[,"Security in Cloud Computing using Hybrid of Algorithms",IJERGS, Volume 3, Issue 5, ISSN 2091-2730,pages 300-305, September-October, 2015.

[3] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking(WiSPNET), Chennai, 2016, pp. 1635-1638, doi: 10.1109/WiSPNET.2016.7566416.

[4] V. D. Orlic, M. Peric, Z. Banjac and S. Milicevic, "Some aspects of practical implementation of AES 256 crypto algorithm," 2012 20th Telecommunications Forum (TELFOR), Belgrade, 2012, pp. 584-587, doi: 10.1109/TELFOR.2012.6419278.

[5] M. A. Muin, M. A. Muin, A. Setyanto, Sudarmawan and K. I. Santoso, "Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations," 2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2018, pp. 137-141, doi: 10.1109/ICITACEE.2018.8576929.