

Enhancing File Storage Security in Cloud Computing using Hybrid Cryptographic Algorithm

Dhawal Darji¹ Siddhesh Jain² Shubham Heda³ Harshil Shah⁴

^{1,2,3,4}Department of Information Technology

^{1,2,3,4}Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract— Cloud computing is an information technology paradigm which is used in different areas like military, educational purposes, IT industry to store vast amount of data daily. Uploading data, downloading data, exchange of information are some of the basic characteristics of Cloud Computing. But there are certain challenges and issues which need to be resolved for providing efficient access to user’s data. Sometimes use of single algorithm in Cloud Computing is not sufficient to provide high level security, so use of multiple algorithms results in more secured platform. In this proposed system AES, blowfish and RC4 algorithms are used to provide block wise security to data. All algorithm key size is 128 bit. Steganography technique is introduced for key information security. Key information contains which part of file is encrypted using by which algorithm and key. All the three algorithms simultaneously work on to encrypt in Hybrid way. Reverse of the same above process is applied to decrypt the file.

Key words: Encryption, Decryption, Cloud Computing, Steganography, Cloud Security

algorithm uses two different keys one for Encryption and another for decryption purpose which gives high level security but more time delay. There are many symmetric algorithms like AES, DES, Blowfish, RC4, etc. which uses block cipher for encoding and decoding of information but results in less secure system. So the proposed system is designed as a hybrid of three different symmetric algorithms namely AES, RC4 and BLOWFISH. 128 Bit Key used is also covered using steganography. Steganography is technique which used in the hiding of a secret message within an ordinary message and the extraction of it at its destination. Only the legitimate user can understand the covered image. The cover image after the once encrypted is further sent to User’s mail id and also will be stored on user’s cloud space. Steganography is used to cover the keys which are being used for encryption and decryption. The advantage of steganography over cryptography alone is that the intended secret message can be decoded but the key here used during the encryption and decryption process is also hidden by this technique which provides high security and integrity.

I. INTRODUCTION

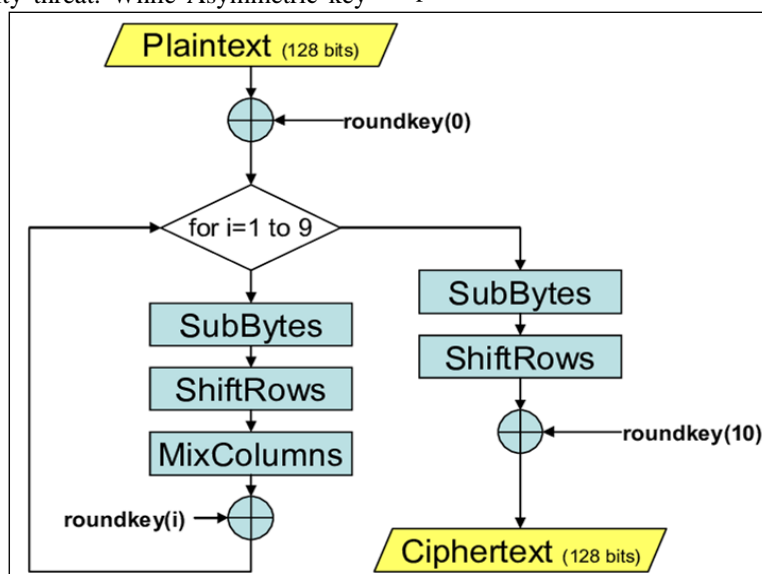
Cryptography is the technique where the input or the original information is translated into unreadable form. The process of encryption converts that plaintext message into cipher text, and decryption converts the cipher text back into plaintext. Cryptographic technique is divide into symmetric key and asymmetric key cryptography where each technique has their advantages and disadvantages respectively. Symmetric key algorithm uses single key for both Encryption and Decryption of files which results in less time delay but increases security threat. While Asymmetric key

II. RELATED WORK

The three algorithms which are being used while implementing the proposed systems are described below:

A. AES (Advanced Encryption Standard):

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. Improved AES algorithm decreased the encryption and decryption time which gives better performance.



The above figure explains the AES algorithm which includes the following steps:

- 1) The Sub Byte step.

- 2) The Shift Rows step.
- 3) The Mix Columns step.
- 4) The AddRoundKey step.

B. Blowfish algorithm:

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. The algorithm follows fiestal network and is divided into 3 main parts:

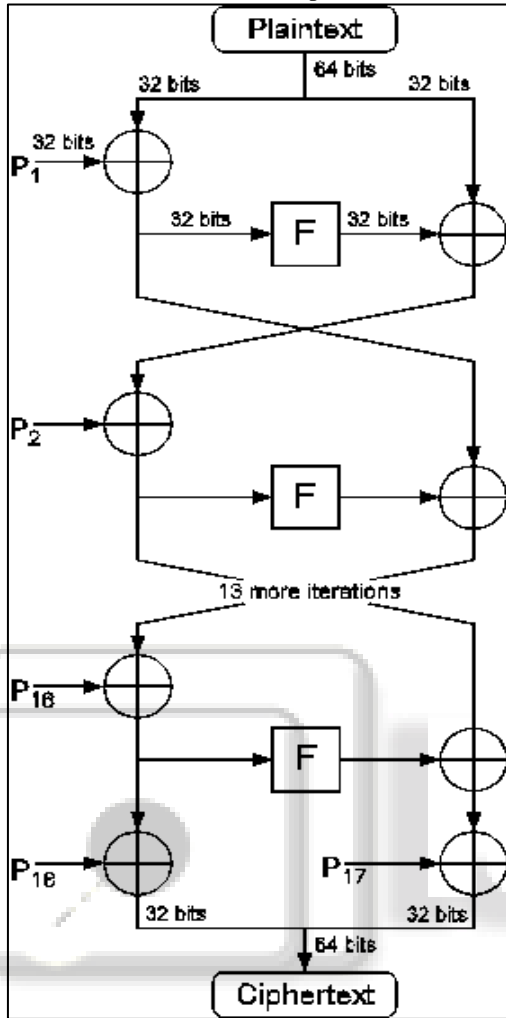


Fig. 2: BlowFish Algorithm

- 1) Key-expansion
- 2) Data Encryption
- 3) Data Decryption

C. Rivest Cipher Algorithm (RC4):

The third algorithm which is to be used is RC4(Rivest Cipher) algorithm as shown in figure 3. The symmetric key algorithm is used identically for encryption and decryption such that the data stream is simply XORed with the generated key sequence.

In the RC4 encryption algorithm, the key stream is completely independent of the plaintext used. An 8 * 8 S-Box (S0 S255), where each of the entries is a permutation of the numbers 0 to 255, and the permutation is a function of the variable length key. The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text.

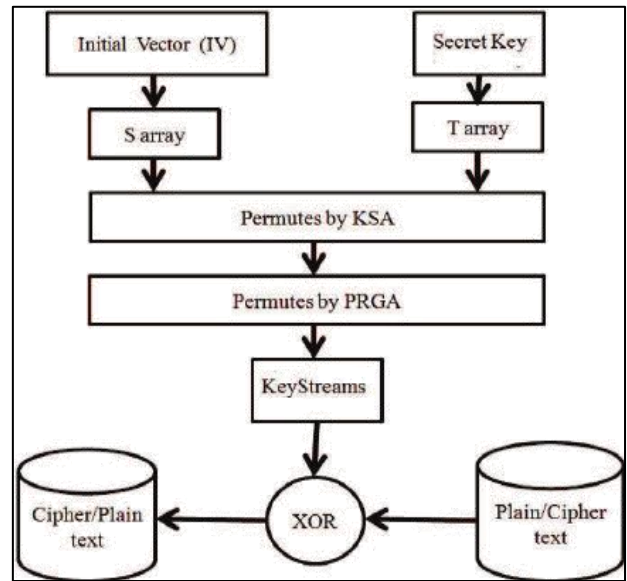


Fig. 3:RC4 Algorithm

III. SYSTEM ARCHITECTURE

The above figure shows the system architecture gives the brief idea about the hybrid cryptographic mechanism. The files to be processed will be split in three ways. The three parts will be encrypted using AES, RC4 and Blowfish algorithm respectively. Encoded file is stored on the cloud server. Keys used for encryption are stored into cover image. The key will be covered into a cover image file using Steganography technique. This cover image file will be emailed to the user as well as stored on the user's cloud space. The user can login at any time via the portal and then use the key provided to him via E-Mail or can retrieve key from his cloud space and use that key to decrypt and view his files. Cloud Computing is an environment where multiple user can simultaneously access file from cloud server. On request of the file the user also gets the steganography image through email which consists of key information. Reverse process is used for decoding of the file.

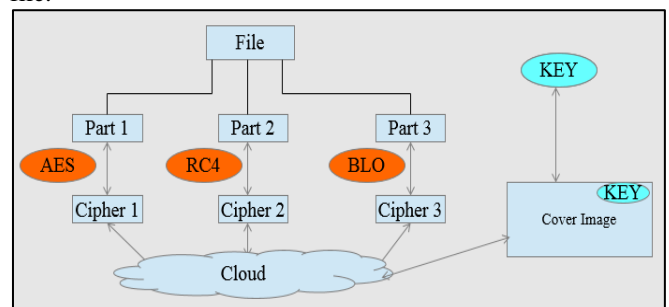


Fig. 4: System Architecture

IV. IMPLEMENTATION

The entire system is based on MEAN Stack which is used for building dynamic web sites and web applications. The MEAN stack is MongoDB, Express.js, AngularJS (or Angular), and Node.js. Because all components of the MEAN stack support programs are written in JavaScript, MEAN applications can be written in one language for both server-side and client-side execution environments.

A. Front-End:

The entire project is build using Angular 5 components, modules and MD Bootstrap for UI designing and angular 5 services for sending HTTP request to the RESTful API sever and for fetching data from the backend. The specific component typescript mentioned below is of the dashboard component that is the redirected homepage post login. The Dashboard Component class has an attribute of the *nodeApiService* which is used to fetch and post data from the backend.

B. Back-End:

ExpressJS-The server functions has a RESTful API server that is build using ExpressJS routing framework for NodeJS. The API server is built using HTTP server functions for Node. Further to allow Cross Resource Access added are the Access Control properties to the server requests. The Express body parser classes are further added. API Interface is also defined for interaction with backend MongoDB.

NodeJS-The server side backend is scripted using NodeJS and the various third party API's are integrated using Node Package Manager (NPM) libraries. Further business logic is written in the latest JavaScript ES6 style of programming. The below pseudo code shows the implementation of the core functionality of file partitioning and encryption of the uploaded file by using the "split-file" node library as well as "file-encryption" library.

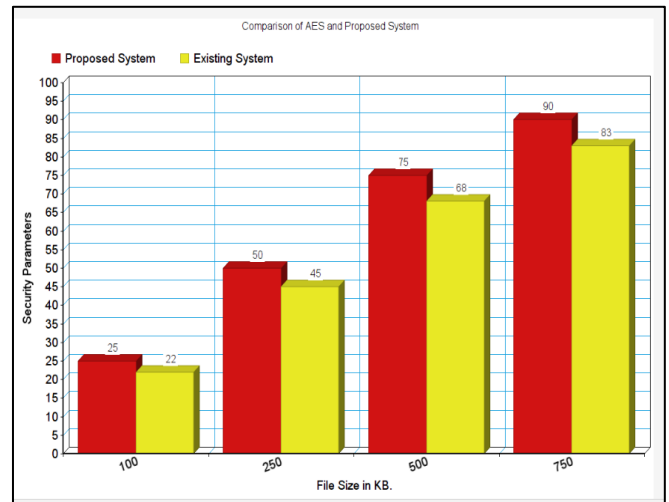
C. Database:

MongoDB The backend database is a completely scalable NoSQL MongoDB that is integrated to our server using Mongoose Libraries for node which uses the concept of Object Relational Mapping (ORM) to perform CRUD operations to and from the Database. Classified as a NOSQL database program with schemas. Mongoose is a MongoDB object modelling tool designed to work in a asynchronous environment. JavaScript can be used in queries ,aggregation functions(such as map reduce) and send directly to the database to be executed.

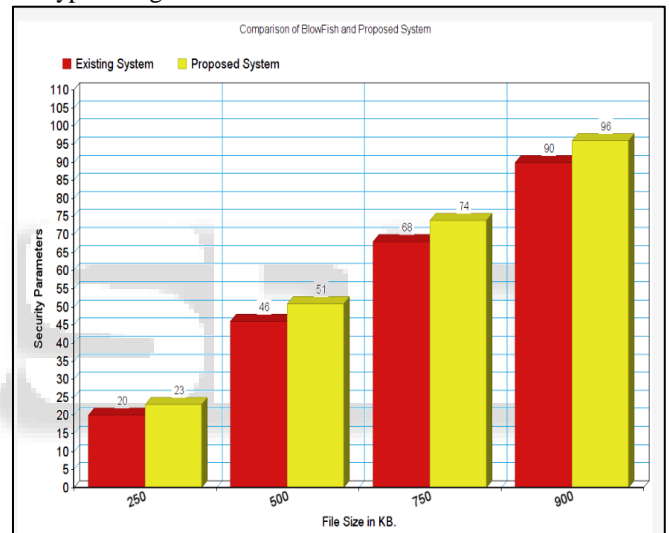
V. RESULT ANALYSIS

In this proposed system AES, RC4 and Blowfish algorithms are used which provides block wise security of data. System is composition of AES, RC4 and Blowfish. All algorithms are symmetric key cryptographic algorithms. They uses a single key for both file encryption and decryption purpose. For hiding key which is being used for cryptographic purpose will be protected using steganography. Javascript language is used for implementation of this system. Security of the system will be calculated with the help of security parameters. File size is given in KB.

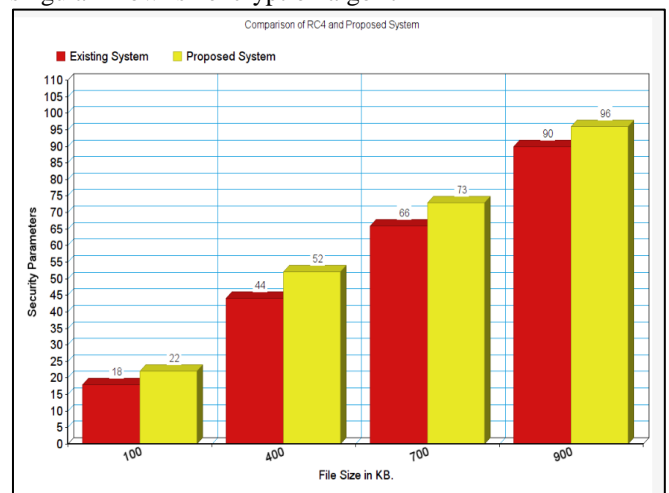
As you can see in the above fig. 5 it takes approx. 8 to 10% more approaches to decipher the hybrid algorithm by using brute force approach compared to a singular AES encryption algorithm.



As you can see in the above fig. 5 it takes approx. 8 to 10% more approaches to decipher the hybrid algorithm by using brute force approach compared to a singular AES encryption algorithm.



From the above fig.6 we can conclude that it takes approx. 10 to 15% more approaches to decipher the hybrid algorithm by using brute force approach compared to a singular Blowfish encryption algorithm



Further it has been observed that it takes approx. 9 to 12% more approaches to decipher the hybrid algorithm by

using brute force approach compared to a singular RC4 encryption algorithm as shown in figure 7.

VI. CONCLUSION

This system represents a unique and more secure as well as efficient mechanism to store a user's sensitive files on their own cloud space without having to worry about data being exposed to other's sharing the cloud space as well as the cloud service provider himself. There are several other cloud storage encryption mechanisms present but hybrid approach towards encryption is rarely seen. The presented application secures the users file by splitting it into various files and encrypting the file by three different block ciphering algorithms namely Blowfish, RC4 and AES which makes the file completely immune to various hacking attacks such as DOS attack, Brute force approach, etc. In usual cases, if a user demands more security for their files on cloud he is charged with multiple additional costs. The presented portal provides the user with maximum security without being incurred with any extra charges as well as letting the user use their own public cloud space such as Dropbox or Google Drive to securely store their files for a negligible cost.

REFERENCES

- [1] Punam V. Maitri ,Arun Verma, "Secure file storage in cloud computing using hybrid cryptography". IEEE WiSPNET 2016 conference.
- [2] Reema Gupta, Tanishka,Priyanka, "Enhanced security in cloud storage using hybrid Encryption". International Journal of advanced research in computer and communication engineering.
- [3] B.Kartikeyan, A.Deepak, K.S.Subalaxmi,"A combined approach of steganography with LSB encoding technique and DES algorithm".
- [4] U.Veeresh,S.P.Kumar, Multi Cloud Architecture to Provide Data Privacy and Integrity IJCERT, Vol. 2, Issue 9, PP 558-564, ISSN 2349-7084 , September 2015.
- [5] M. Nagle, D. Nilesh, The New Cryptography Algorithm with High Through-put, IEEE, ICCCI, pages 1-5, January 2014.
- [6] S.Munjall, S. Garg, "Enhancing Data Security and Storage in Cloud Computing Environment", *IJCSIT*, Vol. 6, ISSN 0975-9646, pages 2623-2626,2015
- [7] Jasleen K., S.Garg, "Security in Cloud Computing using Hybrid of Algorithms", *IJERJS*, Volume 3, Issue 5,ISSN 2091-2730,pages 300-305, September-October, 2015.
- [8] U.Veeresh,S.P.Kumar, Multi Cloud Architecture to Provide Data Privacy and Integrity IJCERT, Vol. 2, Issue 9, PP 558-564, ISSN 2349-7084 , September 2015
- [9] S. Ali Abbas, Enhancing the Security of Identity and Access Management in Cloud Computing using Elliptic Curve Cryptography, *IJERMT*, Volume-4, Issue.
- [10] Kiruthika. R,Jeena.R , Enhancing Cloud Computing Security using AES Algorithm, *IJARCSSE*, Volume 5, Issue 3, ISSN 2277 128X,pp 630-635, March 2015.