Secure Data Storage on Cloud using 3DES and AES Hybrid Cryptography

Vikash Kumar[1] Durgesh Kumar Srivastava[2]
[1,2]Department of Computer Engineering
[1,2]BRCM College of Engineering and Technology Bahal, Maharshi Dayanand University, Rohtak, Haryana, India

Abstract— Cloud registering is utilized in different fields like industry, forces, university, and so forth for different administrations and capacity of immense measure of information. Data set away in this cloud can be gotten to or recuperated on the customers request without direct access to the server PC. However, the huge worry regarding limit of data online that is on the cloud is the Security. This Security concern can be understood utilizing different ways, the most generally utilized systems are cryptography and steganography. Be that as it may, once in a while a solitary strategy or algorithm alone can't give elevated level security. So we are present a new security module that uses a combine of different cryptographic algorithms and steganography. In this future framework 3DES and AES algorithms are utilized to give security to information. Every one of the algorithms utilize 128-piece keys. Our strategy ensures superior safety and insurance of client information by putting away encoded information on a solitary cloud server, utilizing 3DES and AES algorithm.

Keywords: Cryptography, Encryption, Decryption, Cloud Security, Cloud Storage

I. INTRODUCTION

Innovative progressions are bringing about patterns and developments that improve the personal satisfaction. In this quick life where each individual uses a cell phone and approaches the web, the significant worry that the individuals face is with respect to the security of their data present on the web. This security concern is additionally about the record that is put away online on a cloud. This can be comprehended with the assistance of cryptography. Cryptography strategies convert unique information into Cipher content. So just real clients with the correct key can get to information from the distributed storage server. The principle point of cryptography is to keep the security of the information from programmers, on the web programming wafers, and any outsider clients. Non-genuine client access to data brings about loss of secrecy. Security has the characteristics to block or stop this kind of unauthorized access or any other kind of malicious attacks on the data here by securing the users trust. In the distributed computing condition, security is considered to be a critical angle because of the noteworthiness of data put away on the cloud and the various administrations gave to the clients. This information can be classified and incredibly delicate. Consequently the information the board and security ought to be totally solid. It is important that the information in the cloud is shielded from noxious assaults. So for the security of the data, we presented another system in which we are using a blend of various symmetric key cryptography calculation and steganography. In this proposed structure (3DES) and (AES) calculations are utilized to give security to information. AES, 3DES algorithms are joined to hybrid algorithm to accomplish better security. It makes it hard for the attacker to recoup the mystery record of the client.

II. RELATED WORK

Security is an important factor in this digital age. So a huge amount of research is conducted in this domain to protect client's information from any security breach and leaks.

K. Shahade and V. S. Mahale [1] in their investigation exhibited a Hybrid encryption calculation which was a mix of RSA calculation and AES calculation. In their system, the customer makes and stores the RSA private key with himself and besides make a RSA open key while moving the data. In the cloud, the server calls the RSA and AES calculation for encryption of the report and a while later properly store the record on the server.

P. Uddin[2] examined a productive path for data concealing utilizing Text Steganography alongside Cryptography. In this examination, steganography of unadulterated content was planned, with private key cryptography that gives an elevated level of protection. As per the algorithm in the wake of inserting the figure message in the spread content, the content appears customary content.

S. D. Patil[3] proposed a framework for the concealing content in spread pictures utilizing the LSB algorithm and for disentangling utilizing a similar technique. The utilization of information this algorithm can be put away in the LSB of the name picture. And still, after all that, the human eye can't see the concealed content in the picture.

S. Hesham[4] in her examination planned an algorithm to builds the proficiency of the higher Encryption Algorithm. The planned technique lessens the basic way postponement as first algorithm. Contrasted with the first AES encryption/unscrambling algorithm the planned algorithm gives a proficiency improvement of 61% and 29% separately.

A. Advanced Encryption Standard (AES)

The AES calculation is related to Rijndael's encryption. Rijndael is a gathering of encryption calculations with different keys and square sizes. It involves a returns with consecutive exercises, some of them incorporate the commitment of explicit yields (substitutions) and others the mixing of bits (stages). All AES estimations calculation is executed in bytes as opposed to bits. As such, for Advanced Encryption Standard, 128 bits of plain data is considered as a square of 16 bytes These 16 bytes are coordinated in a 4x4 framework for the handling.4

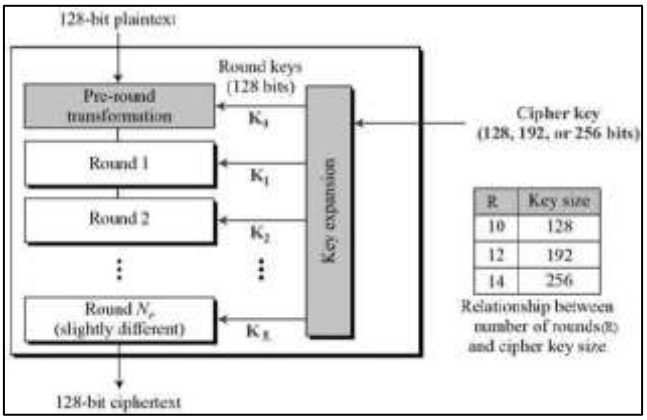

Fig. 1: AES Encryption

AES algorithm is of three kinds to be specific AES-128bit, AES-192bit, and AES-256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256-bits, individually. Rijndael technique was upgraded to acknowledge additional square sizes and furthermore additional key lengths, yet for AES, those capacities were not acquired.

Till the current day, the AES algorithm is used many times and supported on both digital level and physical level. Furthermore, AES comprises of built-in limberness of key length, this allows a certain "future proof" against the process in the ability to perform comprehensive key searches.

1) Triple Data Encryption Standard (3DES)

In cryptography, 3DES is an obtained improved adjustment of DES (Data Encryption Standard). In the Triple DES calculation, DES is used trice to grow the security level. Triple DES is moreover implied as TDES or Triple Data Encryption Algorithm (TDEA).

TDES has following keying choices:

1) All key being unique
2) Key 1 and key 2 being different and key 1 and key 3 is the proportional.
3) Every one of the three keys being identical.

The third alternative structures the three DES. In triple DES the key range is expanded to affirm expansion safety during encryption abilities.

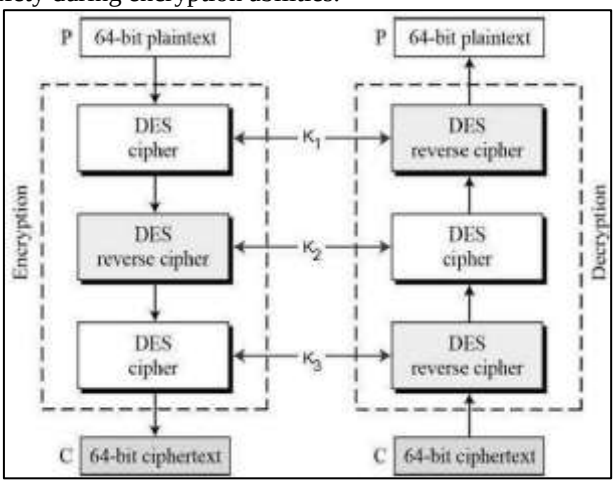

Fig. 2: (3DES) Encryption

TDES is gradually imperceptible from use, it is maximally supplanted by the AES. A broad abnormality is in the computerized installments commerce, which still uses 2TDES and disperses norms on that premise (for example EMV, the ordinary for between activity of "Chip cards", and IC fit POS terminals and ATM's). This ensures TDES will stay as a light-footed cryptographic standard later on.

III. PROPOSED SYSTEM

In the proposed framework, a strategy for safely putting away records in the cloud utilizing a cross breed cryptography algorithm is displayed. In this framework, the client can store the record securely in online distributed storage as the documents are put away in encrypted structure and just the approved client approaches their records.

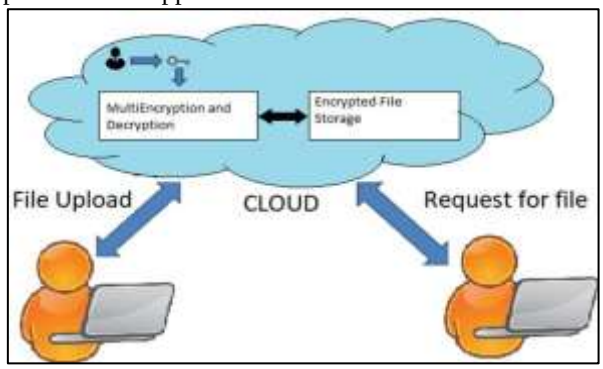

Fig. 3: System Overview

The above figure gives a review of framework. The documents that the client will transfer on the cloud will be encoded with a client explicit key and store up securely on the cloud.

A. Registration of User

For accessing the services the user must first register themselves. During the registration process various data like the name, username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

IV. HYBRID CRYPTOSYSTEM PHASES

The cross breed crypto system use to keep up safety of the records has two levels.

- Encryption Phase
- Decryption Phase

A. Encryption Phase

- On the particular a client, the document is scrambled will be cut in n cuts. Every one of the record cuts is encoded utilizing 3DES key gave by the client to each cut.
- The key will be scrambled utilizing RSA open key
- After encryption, we have scrambled records cuts and the comparing encoded keys.

B. Decryption Phase

A client give n RSA personal keys, as indicated by the quantity of cuts (n) made through the encryption stage. 3DES key is decoded on server end utilizing the RSA personal key explicit the cut.

- with the relating decoded 3DES keys, file cut set away to server are unscrambled.
- The decoded cuts will be converge to generate unique document.

V. PROPOSED CLOUD COMPUTING SECURITY ARCHITECTURE

In order to ensure file security on cloud, the above hybrid cryptosystem is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form. We broadly classify the scheme deployed on cloud in three phases:

- Registration Phase
- Uploading Phase
- Downloading Phase

A. Registration Phase

In the Registration Phase, the client registers himself for transfer and view his records from the cloud server. On the enrollment procedure, a customer send it solicitation to front hub and consequently, front hub doles out the VM of the group hub, which have least burden between other VM's on the system to the customer. Toward the finish of enrollment stage, the customer is enlisted with IP address of relating VM. At whatever point he again gives his solicitation, the solicitation is moved to its relating VM. The encoded documents, scrambled 3DES keys, open RSA keys are put away at his registered VM.

B. Uploading Phase

Steps are as follows in Uploading Phase:

1) Step: 1: The customer will send solicitation to front hub to confirm himself.
2) Stage 2: On successful verification, the front end which send the looking at IP address of the VM against which customer was selected.
3) Stage 3: The records are moved by the client to the selected server (VM).
4) Stage 4: The encryption of moved records is done using the cross breed cryptosystem.
5) Stage 5: The encoded cuts and 3DES mixed keys remain set away in VM's data store.
6) Stage 6: The RSA private keys are send to client lastly they are erased structure the server with the goal that just the confirmed client can see his transferred document.

C. Downloading Phase

Steps are as follows in the downloading phase:

1) Stage 1: A customer send solicitation to front hub to validate himself.
2) Stage 2: On viable approval, the front end which send the relating IP address of the VM against which customer was enlisted.
3) Stage 3: A customer is transfer n RSA private keys to the relating n cuts.
4) Stage 4: A RSA private keys is decode that comparing scrambled 3DES keys or encoded cuts is unscrambled by 3DES keys.

VI. CONCLUSION & FUTURE SCOPE

The primary point of this framework is to safely store and recover information on the cloud that is just constrained by the owner of the information. Distributed storage issues of information security are explained utilizing cryptography and steganography methods. Information security is accomplished utilizing 3DES and AES algorithm. Key data is securely put away utilizing LSB strategy (Steganography). Less time is used for the encryption and disentangling process using multithreading framework. With the help of the proposed security framework, we have accomplished better data dependability, high security, low deferral, approval, and mystery. Later on we can add open key cryptography to avoid any attacks during the transmission of the data from the client to the server.

REFERENCES

[1] A. K. Shahade, V.S. Mahalle, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE, INPAC, pp 146-149, Oct .2014.
[2] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology, Network, Vol. 13, Iss. 15, 2013.
[3] Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam," Secure File Storage on Cloud using Hybrid Cryptography",ICSE, Vol. 7, Jan 2019.
[4] 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.
[5] Srinivasarao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011.
[6] Swarna C, Marrynal S, Eastaff," Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm"JARAS, Vol 5, march 2018.
[7] 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.
[8] S.Rajendirakumar, Dr.A.Marimuthu, "Cryptographic Algorithms used in Cloud Computing – An Analysis and Comparison", International Journal for Research in Applied Science & Engineering Technology, Vol 6, Iss. 1, 2018.
[9] R. T. Patil and P. S. Bhendwade , "Steganographic Secure Data Communication",IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.
[10] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm", in Proc. IEEER egion 10 Conference, pp. 1-4Jan. 2009.

