An Efficient and Secured Data Loss Prevention using Hybrid Cryptosystem for Secure Data Storage

V.Krishna Reddy, A.Devi Chandana, E.Sri Pujitha, M.Pranitha Shravani

Abstract— Cloud computing has transformed into an irreplaceable bit of a substantial part of the private, open affiliations that are being used for data accumulating and recuperation. There are various utilization of circulated processing and furthermore comprehensively used in the exceedingly mystery national organizations that are available like military ,treasury to secure the private information. The circulated processing for example like Google drive, Amazon Web Service and Microsoft Azure are important for affiliations and end-customers. Using the Cloud by making sense of and its organizations, affiliation/end-customers can store their data. There are diverse challenges amid saving affiliations incredibly arranged records in servers. Therefore, the goal of this paper is to give an abnormal state structure to a capacity framework providing security and individual protection. In spite of the fact that servers are profoundly secured and protected against unapproved access, there are episodes where private documents put away on servers are gotten to by the upkeep staffs. Subsequently this examination paper gives early on structure to completely assurance of records put away in the server by utilizing Hybrid Cryptosystem In this paper we are finding the touchy data from the document and it ought to encode by the deletion encoding after that it's scrambled by the utilizing MD5 for residual information it ought to scrambled by the sha-1 at that point joined the information and put away into the cloud.

Keywords — Cryptography, Encryption, Decryption, Security

I. INTRODUCTION

The cloud is well known to store information and documents because of the low costs, less support and straightforward entry from any area. Aside from the private and open associations, taxpayer driven organizations are searching for cloud based capacity and administrations for their secret information stockpiling. Each cloud supplier like Microsoft Azure, IBM, Amazon Web Services (AWS) and numerous others have given their very own method to encode and decode the information. The distributed computing is broadly utilized in private and open administrations associations for putting away colossal measure of information which can be made accessible from any area. The utilization of cloud is found in industry, military universities, and private associations. The information put away on the cloud is open by client confirmation however for secret access numerous layer of security is executed. The calculation of this different layer security is reliant on the dimension of protection. To give the answer for various dimensions of security, cryptography and steganography systems are well known. Different calculations must be fused to improve the dimension of security in information stockpiling. New strategy, utilizing symmetric key cryptography calculation and steganography is proposed in this work.

II. LITERATURE REVIEW AND EXISTING SYSTEM

Data Security Issues [5] are essential issue in the present structure. Due to the open and multi-tenant characteristics of the cloud, the traditional security segments are never again fitting for applications and data in cloud. A portion of the issues are as following:

1. As a result of the dynamic flexibility and organization and territory straightforwardness features of the dispersed registering model, a wide scope of utilization and also data of the cloud arrange has no settled system and security restrictions. If there should be an occurrence of security break, it is hard to withdraw an explicit resource that has a hazard or has been jeopardized.

2. According to profit movement models of the Cloud handling, resources and cloud organizations may be controlled by different providers. As there is a troublesome security issue watched, in such condition ,it is difficult to send a bound together wellbeing exertion.

3. Because of the transparency of the cloud and sharing a virtualized assets by using a multitenant environment, client information might be gotten to by other unapproved clients.

The word cryptography implies changing the message information into a mixed code which can be recovered back on open system. Cryptography strategy anchors the delicate data in unbound transmission systems and which can be perused by planned beneficiary. A cryptography calculation needs a key alongside a message of any configuration to frame the figure content. The dimension of security of figure content relies upon the quality of cryptographic calculation and protection of the cryptographic key utilized. Subsequently the principal dimension of security has been given. Further security can be enhanced utilizing one more Data concealing method, Setganography. In this framework that we proposed AES, RC2, DES calculations are utilized

Revised Manuscript Received on 14 February, 2019.

Dr. V.Krishna Reddy, CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India. 522501. (Email: vkrishnareddy@kluniversity.in)

A.Devi Chandana, CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India. 522501. (Email: chandanareddyalla31@gmail.comt)

E.Sri Pujitha, CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India. 522501. (Email: pujithaedara@gmail.com)

M.Pranitha Shravani, CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P, India. 522501. (Email: masamsetty.pranithashravani@gmail.com)

to give doubled shrewd security to information. Key data security is actualized by utilizing LSB steganography system. The reason for Key data is to choose connect between accessible calculation and key record encryption. By utilizing this procedure the document is divided into three sections and each part utilizes one of a kind calculation system. Multithreading is utilized to scramble all aspects of record all the while for enhancing the execution. LSB system is utilized to embed Data encryption Keys into cover picture. Substantial client gets an email with Stego-Image of the key. Turn around procedure of encryption is connected for record decoding reason. Symmetric key cryptography calculations are as follows AES, 3DES, DES, IDEA, ECB,BBRA, CBC and blowfish. These calculations achieved abnormal state security however increment delay for information encode and disentangle. Steganography shroud the mystery information presence into envelope.

In this system presence of information isn't unmistakable to all individuals. Just legitimate collector thinks about the information presence. Picture steganography method is utilized to create high security for information. Mystery information of client stow away into picture record. In the wake of including content into picture record it would appear that typical picture document. DES calculation is utilized for content encode and unravel. Favorable position of picture steganography method is giving security to content.

Three piece LSB method utilized for picture steganography. We can cover up gigantic measure of into picture utilizing LSB steganography strategy. AES is a symmetric key cryptography calculation. It bolsters 3 sorts of keys. For a 128 piece key generation it requires 10 rounds where as a 192 piece key requires a 12 rounds and 256 piece key requires 14 rounds [6]. In enhanced AES calculation encryption and unscrambling time is decreased. The advantages of changed (AES) calculation is gives a good execution regarding delay [1]. DES has an application of a solitary key for writings encode and decipher. Size of a key is 128 piece. In this calculation numerous means are executed haphazardly so ill-conceived client can't figure the means of calculation. Give a high and efficient throughput is one of the upsides of a symmetric key i.e, two key cryptography calculations. [4] Improved DES calculation utilizes a 112 piece key size for information encrypt and disentangle. Key age process is finished utilizing irregular key age system. It gives security to information. Disservice of this calculation is fundamental most extreme time for changing over information into figure content since it works on single byte at once.

III. PROPOSED SYSTEM & RESULTS

The arrangement of the deviated cryptography is improved with the extra layer of security by consolidating AES, DES, RC6, ECB, CBC, Triple DES calculations. The proposed framework is a procedure improvement for record security issues away frameworks. Same idea as of distributed computing is actualized with new strategy and technique, where client can store information and can get to it utilizing proposed framework. The general proposed framework structure is appeared as beneath figure 1.

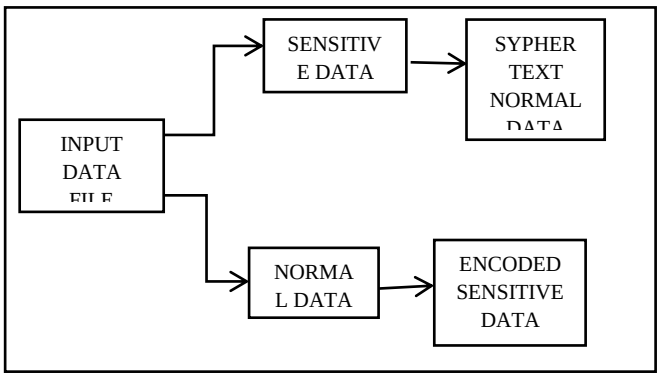

Fig. 1: Proposed Storage Architecture

The encoding of the transmission files and pictures square measure keep victimisation of the steganography technique as shown within the figure 2.

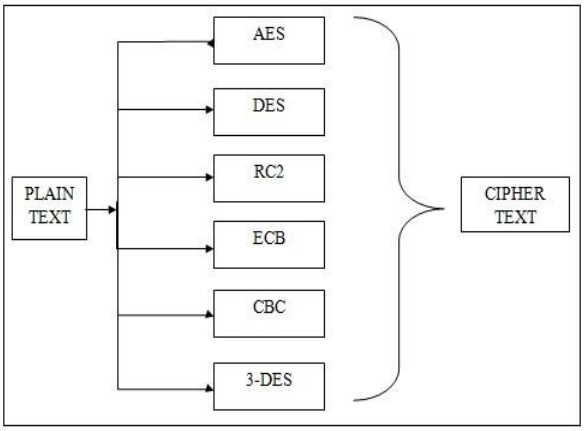

Fig. 2: Encryption Algorithm for each data part.

In this proposed system AES, DES, RC2, ECB, CBC, 3DES estimations are used to give doubled adroit security to the data. LSB steganography strategy is been introduced for the key information security. A Key information contains which part of the record is encoded is used by which count and the key. Document should be divided in terms of 3-6 sections according to client input. Every single piece of document is scrambled utilizing distinctive calculation.

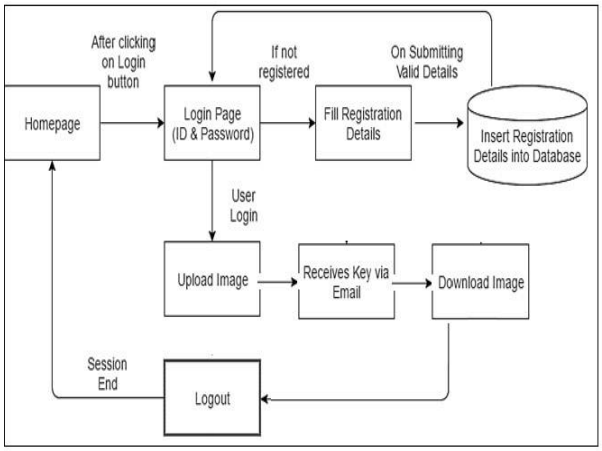

Figure 3: Overall System Architecture

All parts of the data are encoded in the same instance with the help of multithreading technique data encryption Keys are implanted into picture which is used as a key, using LSB procedure. Stego-Image is sent to considerable authority using mail. For archive unscrambling reason switch strategy of encryption is associated. Figure 3 gives an outline of framework design. With the end goal to guarantee document security on capacity framework, the above mixture cryptosystem is sent on server/cloud/nearby framework. The plan sent is in three stages as recorded.

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

The periods of execution are clarified underneath.

1. Registration Phase:

In the Registration Phase, the end clients enlist with the end goal to transfer and view records to/from the capacity server.

2. Uploading Phase:

The archives are exchanged by the end customers to the selected server. The encryption of exchanged records is done using the creamer cryptosystem. The private keys i.e. stego-picture is sent to customer over mail with the objective that approved customer can see exchanged record.

3. Downloading Phase:

On fruitful validation, the client gives the private key i.e. stego-picture for the relating n cuts. The private keys decode the relating encoded cuts. The unscrambled documents are converged to produce unique record. The decoded document is downloaded and saw at client end.

Erasure Encoding:

At whatever point the information is been transmitted , the danger of losing parts of the data because of the blotch occured in a basic transport mode. In web , we adapt to the issue that utilizes specific conventions like for example, TCP/IP that is dependend on a back-channel to ask for the absent or a ruined information bundles. In any situation, in numerous events there is no such back-channel and we need to utilize some type of forward blunder remedy (FEC). Using FEC data is encoded so the recipient can viably interpret the message with high probability even inside seeing erasures (distribute) and data contamination (e.g. flipped bits). Annihilation Coding is one kind of forward oversight modification where data is sent over an indicated cancellation channel (see Section 2.1 for increasingly unpretentious components). On the sender side, the message of length k is encoded into a code articulation of length n, where n > k, which essentially incorporates n − k uniformity pictures. At the point when the message is encoded the code word is sent over the annihilation channel and parts of the code word accomplishes the recipient. The authority can decipher the maybe divided code each word and join the principal message accepting "enough" data is accessible and available. This technique is only an outrageous depiction that needs various basic and vital focal points, which should and will, consistently present in this and the going with region. Eradication codes are utilized in various applications and this is only a deficient rundown of such. The NASA and ESA set forward a suggestion of utilizing Reed-Solomon (RS) codes (portrayed in Section 3) for the information transmission in the majority of their profound space missions [8]. Besides, deletion codes are likewise utilized in satellite correspondence; truth be told, in the event that you watch computerized TV, odds are great that the solid information transmission is accomplished through eradication coding. Eradication codes especially exceed expectations in communicates situations where no back-channel is accessible or exceptionally costly. Indeed, even the Compact Disk (CD) utilizes RS codes to shield the information from scratches at first glance and the these days extremely mainstream QR-codes utilize comparable codes to ensure that the substance can be gotten to, regardless of whether the QR-code is harmed. Closer to the use of eradication codes in conveyed stockpiling frameworks is the following use case. Assault Level 6 utilizes RS-codes to endure any two plate disappointments.

IV. CONCLUSIONS

Information Security and Privacy of information put away in have loaded with difficulties. Nonstop researches are been proceeding in order to enhance the information in terms of security. This paper presents half breed security calculations utilizing the symmetric key. This process and methodology help in decreasing the encrypt and unravel the time and henceforth help in enhancement of the execution to put away extensive information documents in a significantly tied down condition. Since the key is been tied down in this way it more likely than not gotten to by the endorsed customer. The estimation is been created and furthermore prepared on the cloud server with the objective that the data improvement development is constrained. The arrangement proposed in this exploration gives extra layer of security by joining AES, DES, RC6, ECB, CBC, Triple DES calculations to awry cryptography. This strategy applies the key data on information stockpiling (server stockpiling framework).

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.