Information Security in Cloud by using Enhanced Triple-DES Encryption Algorithm

Gudapati Syam Prasad, Dande Lakshmi Praneetha, Seelam Srivalli, Bhavanasi Venkata Sukesh

Abstract*: The purpose behind triple des encryption is to allow count on encoded data. Cloud computing is the most widely emerging technology in present world. Many domains used this technology in present world. In this paper, the proposed system provides the integrated security in the cloud for secure the data in cloud storage.

***Index Terms*: cloud computing, cryptography, triple des, cloud security, virtualization.**

I. INTRODUCTION

Cloud computing marks another development towards IT framework dematerialization; and gets a great deal of thought, both in manifestations and among clients. Regardless of whether they appreciate it or not, different individuals use Cloud computing associations for their very own extraordinary necessities. For instance, different individuals utilize easygoing correspondence zones or webmail, and these are cloud associations. Clients of Cloud computing are getting self-organization, ergonomics and straightforwardness. This new viewpoint renders the Internet a wide storeroom where assets are all around made, satisfactorily shared and accessible to everybody as associations. Virtualization is among the movements used to give these cloud associations. Virtualization is a lot of apparatus and programming strategies that concede to run diverse working structures in the interim on one contraption totally separate from each other. Thusly, a working framework called "host" is displayed on a machine and has working structures "guests" or "virtual machines". Virtualization and affiliation can upgrade server farm the board, lessening the measure of machines by overhauling asset usage and empowering high accessibility. Cloud security challenges are an issue for a couple of specialists; first need was to concentrate on security, which is the best worry of affiliations altogether thinking about a move to the cloud. In any case, the social event of the cloud applies just if security concerns are guaranteed. The ask for eventually is by what means may we ensure security in cloud field. The reasonable response is the encryption, an encryption that is absolutely homomorphic, and gifts to enroll over blended information without unraveling them. This sort of encryption was proposed unprecedented for 2009 at Stanford University by C. Gentry [1]: first cryptosystem empowering to perform discretionary relies upon encoded information without unwinding them. Neglecting the manner in which that the proposed course of action has a few downsides (too exorbitant to the degree memory and incredibly moderate as for speed), at any rate has made arranged for various examinations on this sort of homomorphic encryption. Our work is according to this work, explicitly around those of Sai Deep Tetali, who proposed MrCrypt [2]: a structure that guarantees secret of information by executing managing customers on figures, this by utilizing basically almost the whole way homomorphic encryption estimations.

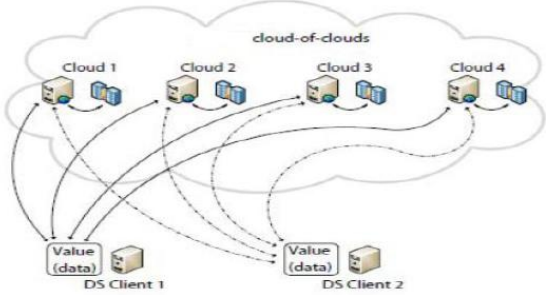

Fig.1 Data Partion Architecture Diagram

II. RELATED WORK

In paper [3] shows completely homomorphic encryption plot engages to work unmistakable sorts of development on encoded information. In this paper [3], presents a stir setting up the information on different focus fixations by parallel dealing with the encoded information utilizing absolutely homomorphic encryption. In this work, they utilized the high society's estimation to perform FHE. The parallel administering will reduce the time taken to play out the related activities on blended information in a cloud space. The totally homomorphic encryption is performed on the unquestionable fixations to diminish the supervising time. This work is done on a private cloud utilizing sensibility's figuring. In paper [4] demonstrates client stores their information on cloud and they need to shield those information from the standoffish assailant or unapproved clients. So clients need security to their information that is kept an eye on cloud. On passed on gathering, security is a one of the troublesome issue. There are a couple of encryption strategies are exist, utilized for secure the client's information that is affirmed cloud. A couple of frameworks look like Full Disk Encryption and Fully Homomorphic Encryption. SamjotKaur, Vikas Wasson presents a work on homomorphic encryption and they used the Diffie Hellmanfiguring for symmetric key assention. Diffie

Revised Manuscript Received on March 10, 2019.

Dr. Gudapati Syam Prasad, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.
Dande Lakshmi Praneetha, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.
Seelam Srivalli, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.
Bhavanasi Venkata Sukesh, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.

Hellman figuring is a key exchange check. Right when two affirmed gatherings need to give each other, this estimation make session key between them. In addition, it in like way makes "HMAC" for the customer's data legitimacy and "One Time Password" for progressively crucial security. In paper [5] distributed computing gives the on-ask for relationship to the customers of cloud. Customers are charged by payper-use show up. In this paper, Mbarek Marwan, Ali Kartit and Hassan Ouahmane present a work subject to the homomorphic encryption strategy to certify the client data. Additionally, they likewise show playing out the number juggling works out (choice and augmentation) on mixed data. RSA figuring is used to shapes the development depend on mixed cloud data in light of the way in which that RSA is a multiplicative homomorphic encryption. Paillier encryption is used to apply homomorphic improvement undertaking on encoded data. In [6] this paper demonstrates a restorative application. They used the homomorphic encryption structure to allow estimation on encoded cloud data without unscrambling the figure . Moreover, other than they portray about homomorphic encryption occupations on encoded data; it will give security data sharing and demand of data on cloud condition. In this they show lacking homomorphic checks to perform math attempts on encoded cloud data. This proposed supportive undertaking is used to process the fragile patient's data that is confirmed on cloud.

III. SECURITY

The cloud computing did not bring just focal points, yet moreover different dangers. As indicated by NIST, security, interoperability and convenience are as far as possible to progressively indisputable assurance of cloud. Security issues of passed on preparing the most examined can be collected into four basic game plans [7]:

• **Cloud foundation:** wires concerns about virtualization, putting away and system vulnerabilities correspondingly as the code and programming energized in the appropriated enrolling, and the physical security parts of the server farm.

• **Data:** merges the worries over information uprightness, receptiveness and gathering and client security.
• **Access**: worries around access to the cloud (affirmation control, get to underwriting), encryption of correspondence, and the main gathering of client personality.

• **Compliance:** cloud must settle two or three issues concerning the control (security surveying, information confinement and prominence).

It is indispensable to meet the security necessities at every estimation so as to guarantee information security in thecloud (gathering, uprightness, accessibility and non-refusal). Similarly, one must guarantee the adequacy of these measures, their life, their protection from ambushes and their centrality to client needs and heads Cloud.
Ten scattered figuring obstructions were seen by a get-together of University of California at Berkeley research [8] (association receptiveness, information security, blocking, programming licenses ...).
The Cloud Security Alliance (CSA) sees thirteen districts of weight on the security of scattered handling [8]. Information insistence and insurance in the cloud looks like standard information security and secret. Security must be consolidated at every part of the information life cycle. Because of multitenancy, confirmation and riddle of information in the cloud end up unequivocal.

IV. MULTI CLOUD ARCHITECTURE

The totally homomorphic encryption structures [9] are dull. Considering the evaluation of one entryway asking for a restore, the run-time will be crucial in like manner as the getting ready of security parameters. A recommendation of an about FHE scheme based organizing for engaging the evaluation of any cut-off and managing mixed data is tended to in Figure 2. In our proposed game plan, the ace connection repartitions the managing among the servers to join the examination method for any capacity.

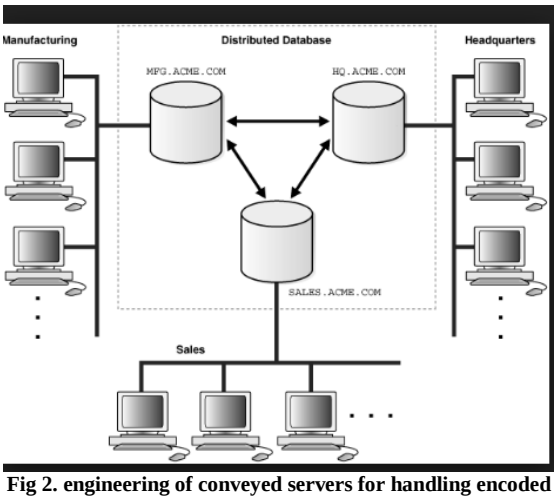

Fig 2. engineering of conveyed servers for handling encoded information

Here, we are giving a high leveled course of action plot using arranged Servers. Duplicating a veritable client, there by sullying the whole cloud. This prompts impacts different clients who are sharing the sullied cloud. There are five sorts of issues raise while examining security of a cloud Data Issues, Privacy issues, Infected Application, Security issues and Trust Issues. Homomorphic cryptosystem acknowledge fundamental occupation with these issues. This calculation System will about allow accomplishing a FHE, and thusly colossal number of activities including additions and extensions can be performed. For example, in Fig A, Client 1 asks for the postponed outcomes of a given breaking point, expect $f(x) = ax^2+bx+c$. For this situation the breaking point portions are encrypted and divided into several anomalies relying on the measure of endeavors (Multiplication and advancement), and will be organized uninhibitedly on N specific servers, commensurate to the measure of augmentation practices.

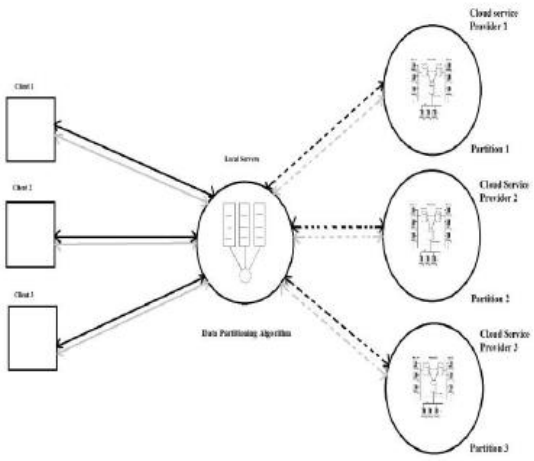

Fig 3. Proposed architecture to secure data using Homomorphic encryption

Finally the outcome is sent back to a Central Server to be sent to Client 1 and after that decrypted. The good position is that no longer chipper text after encryption not in the slightest degree like the standard technique. The keys are feasibly managed and progressively unmistakable security is kept up since is it difficult to inspect material data in appropriated structures. In the cloud the N servers includes hypervisors hosting particular virtual machines which help overhauling the reaction time and develop the measure of the included computational segments in the passed on framework. In this proposition, we assess the additional estimation of the passed on structures in preparing practices asked for by customers. The course of action of homomorphic encryption is dispatched inside the servers and this can be reasonable and help enhancing the security of the cloud like gathering of information and execution.

An Integrated Security System for cloud storage

Step: 1 admin login.

Step: 2 add files to the cloud and encrypt the every file and generate the key for further communication.

Step: 3 for the key generation and encryption file we have used Triple Des Encryption algorithm. The algorithm steps as follows.

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the cipher text.
- Decryption of a cipher text is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Step: 4 User Registrations and Login

Step: 5 Search for File in cloud.

Step: 6 File found.

Step: 7 to download the file, admin have to give the permission to user and admin have to sent the key to the user mail.

Step: 8 File downloaded.

V. RESULT ANALYSIS

Triple DES is much more secure than single DES and any other cryptographic algorithms .It is used for securing the information and it is often used in the cloud security. It is applied three times than a normal DES algorithm. We can see the results in the below tabular form.

FACTOR	3-DES
KeyLength	168 bits(3 key), 112 bits(2 key)
Cipher Type	Symmetric Block
Block Size	64 Bits
Developed	1978
Weakness to hacking	Brute Force Linear Cryptanalysis
Security	Inadequate
Possible Keys	2^112
Rounds run through Algorithm	48
# Keys	2 or 3

Fig 4: Analysis on 3-DES

Algorithm	Memory(KB)	Time(Sec)
Homomorphic Encryption	20.5	11.8
3-DES	15.5	8.6

Table: 1 Comparison between homomorphic and 3-Des in terms of memory and time.

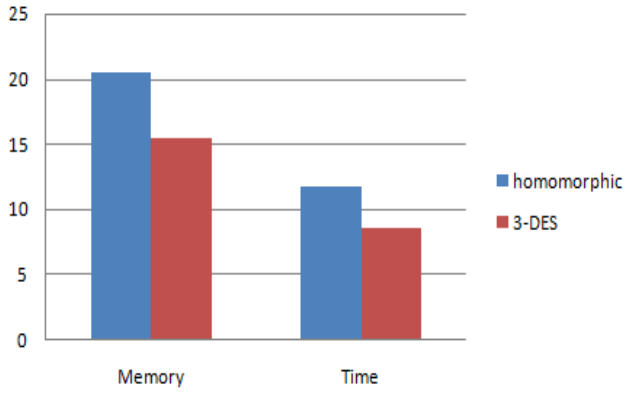

Fig 5: Bar Graph Showing Comparison Between homomorphic and 3-Des in terms of memory and time.

VI. CONCLUSION

In this paper we take a gander at the need of Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES. We endeavour to exhaust down various sorts of Triple DES as present today, under the two general groupings unequivocally almost the entire way and absolutely in integrated security system.

REFERENCES

1. Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In *2005 international Conference on information and communication technologies* (pp. 84-89). IEEE.
2. Salama D, Kader HA, Hadhoud M. Studying the effects of most common encryption algorithms. International Arab Journal of e-Technology. 2011 Jan;2(1):1
3. Kumar A, Jakhar S, Makkar S. Distinction between Secret key and Public key Cryptography with existing Glitches. Indian Journal of Education and Information Management. 2012 Sep 1;1(6):392-5.
4. Marwan, M., Kartit, A., & Ouahmane, H.(2016, October).Applying homomorphic encryption for securing cloud database. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt) (pp. 658-664). IEEE.
5. Bensitel, Y., & Romadi, R. (2016, May). Secure data storage in the cloud with homomorphic encryption. In 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech) (pp. 1-6). IEEE.
6. A. Ait Elmrabti, A. Abou El Kalam and A. Ait Ouahman , "Les defis de Securitedans le Cloud Computing, Problemes et solutions de la securite en Cloud Computing," 2012.
7. Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: A berkeley view of cloud computing. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS. 2009 Feb 10;28(13):2009.
8. Alliance, C. (2011). Security guidance for critical areas of focus in cloud computing v3. 0. Cloud Security Alliance, 15.
9. C. Gentry, "A fully homomorphic encryption scheme," Doctoral dissertation, Stanford University, 2009.