Multi-Cryptosystem based Privacy-Preserving Public Auditing for Regenerating Code based Cloud Storage

Rinku Kumar
M-Tech Computer Sc. & Engineering
Sagar Institute of Science & Technology
Gandhi Nagar, Bhopal, M.P, India

Rajit Nair
Assistant professor
Sagar Institute of Science & Technology
Gandhi Nagar, Bhopal, M.P, India

ABSTRACT
The huge amount of data coming from different outsource in cloud storage is to be regenerated by a couple of keys and it can be regenerate code using partial keys for securing the original data privacy against the TPA (Third party Audit). It uses proxy server to maintain the file in distributed storage system. A third party auditor(TPA) and semi trusted proxy server, both are implement to the data integrity checking and code regeneration in case of failed authentication and data block. So the design of framework structure system to access the huge amount data requires more cryptographic encryption system.

The proposed work is used to design framework structure engineering with high cryptographic encryption technique. In cloud storage we require protection from different kinds of corruption, fault tolerance on data cordiality check in regenerating code based. It is very crucial matter to secure the data in cloud storage which uses working framework predominance of authorization values in four areas (User, TPA, Proxy Server and Cloud Server). The cryptography technique is used to kept secure information transforming and downloading inside specific location in cloud storage. Hence a new procedure is introduced here to checked data integrity with help of TPA (Third Party Auditor). The main purpose of auditing procedure is keep secure own data. This proposed auditing scheme makes use of either AES or DES algorithm for data block encryption. This works does not only introduce cloud related issues but also invents underlying information need to security on the cloud server.

General Terms
Security, DES Encryption algorithm, AES Encryption Algorithm, Homomorphic Encryption Schemes, Repair Data block, Regenerating code.

Keywords
Cloud Storage, TPA, Privacy Preserving, Public auditing, Proxy Server, data Integrity, Third Party Audit.

1. INTRODUCTION
According to the NIST definition, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider Interaction" [10]. A cloud is a type of parallel and distributed system that consists of a collection of interconnected and virtualized computers which are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements (SLAs)[9]. End-users do not own any area of the infrastructure. They simply use the specific service available through cloud computing paradigm and pay for the used services. Only cloud service provider are own the area of the infrastructure. Distributed storages system propose good management, Specialized, new inventive and open the door for changes the way of business organization. In case of cloud administration, these are following Oracle cloud, Office 365 and Google Engine. In this cloud administrator have the security inside the cloud storage device. The first of all the implement of distributed storage device has ensured security challenge between cloud service provider and clients. Many cloud service suppliers including Google, Microsoft, yahoo, IBM, and rack space etc. The main issue is these cloud service supplier to protect the information inside or outside in distributed system environment. Without verify no anyone could be gotten user secret data in the distributed cloud storages framework, CPU, memory stage and application. Data integrity is one of the best word itself defines the "wholeness" and "completeness" of database equally integrity of data storage. It is the fundamental needs of the information technology on base of the information storage in distribute system. It is verify the validity, regularity and consistency of the data or information. It is one of the best techniques of access data or information in a secure way the load in cloud storage device. It can be retrieved or reclaim in the same layout and stored later. Data security means data protection; data availability, data location, data privacy and data secure transmission on demand of user. Data auditing is introduced in cloud storages to main purpose of secure data storage, it is a procedure of verification of data owner which can be carried out either by the user himself (data owner) or TPA. It used to maintain the data integrity stored on the cloud.

2. LITERATURE SURVEY
Jain Liu, Kun Huang, Hong Rong and M. Xian[1] July 2015, They are introduce a proxy server to find the solution of failed authenticators or error server in absence of data owner to regenerate data block code and authentication. We design a novel public verifiable authenticator to generate a couple of keys. In this scheme can completely release data owners from online burden. It uses the public key based homomorphic linear authenticator based on BLS signature. Which can ensure the integrity and privacy of data stored in the cloud storage in this model. Swapnali More, Sangita Chaudhari (2016) [2]. They are proposed system to verify the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data using AES algorithm, SHA-2 for integrity check and RSA signature for digital signature calculation. This system is support privacy preserving public auditing protocol which makes use an effective audit scheme According to Subashini and Kavitha, V. (2011), [3]. In this paper a survey of the different security risk of data in cloud environment. The main security issue in service delivery models such as SaaS, PaaS, IaaS of a cloud system. But detail

survey security issues in SaaS related to Data security, network security, data locality, data integrity, data access, authentication and authorization. As per Zissis, D., & Lekkas, D. (2012) [4]. They introduce a trusted third party checking validation data or information under the cloud computing with quality of security. They are used to a special public key infrastructure in cryptography working with SSO and LDAP model. According to Cong Wong and Sherman S.M Chow [5]. In this system work in a secure data storage supporting privacy preserving-public auditing with help of TPA. The TPA performs audit procedure, if Data owner stay online and demand the audit. This system protects the data against attackers to access remote storage device. As indicated by Schoo, p. Fusenig, and Souza [6] cloud computing is just like a big server to connect the service provider with users with new security challenges as considered in SAIL for guaranteeing genuine or must utilization of cloud systems administration assets and to prove reproach. According to Ramgobind, S., Eloff, M.M., Smith, E. (2010, August) [7]. This system model provides protection of information or data from different type of virus, corruption data and data crash. Cloud computing is just a stage where people and organization utilize the internet and interminable equipment of information and programming with security. Due to this vast majority of business is involving this system. S. Arasu et al[8]. In this system model has proposed a method use the technique key Hash Message Authentication code (HMAC) with homomorphic tokens to increase the preformation of the TPA. It verifies data integrity between two users in case of data transmitted that agree on a shared secret key.

3. PROPOSED METHODOLOGY

3.1 Existing System

Private information in cloud server by the help of public auditing to solve the regeneration data blocks code and authentication of failed server worthiness the absence of data owner. In this model some problems are created than after make a new implement. Its name is third party auditor (TPA) and proxy. It avoids on-line burden on the cloud server. A third party auditor takes the responsible for check integrity of all private information store in distributed storage system. In which the purity or wholesomeness checking and regeneration are implemented by a third party auditor and a proxy separately on someone of data owner. Our plan completely release data owners from online for the regeneration of failed data blocks and trust the quality of being worthy at faulty servers and it provides the prerogative monopoly to a proxy for the reparation. To introduce of proxy, this is prerogative monopoly to regenerate the authentications into the traditional public auditing system model.

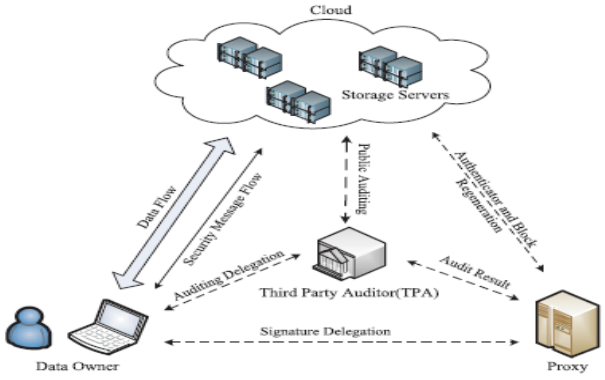

Fig.1 Existing System model

3.2 Problem Identification

- Private data coming from different source directly store in single cloud server by cloud service provider. Hence attacker can be crack private information easily.
- This system is used to simple cryptosystem in cloud server. Hence attacker can be easily crack private information.
- This system is allowed to private data to upload and download from cloud server to pliability manner. Hence data management scheme goes through a dynamic hierarchical service chain and a complex. So it does not used generally behave in conventional environments.

3.3 Research Objectives

- We can't blindly trust to TPA or Proxy server. It can be disclose our information or data, if TPA (Third party auditor) knows that where is private information store in cloud server. Hence to show critical issue of security for the data owner\user's to trust on the cloud service provider.
- In this proposed work show that the challenge of high security provides to users to store own private information in cloud server. This research work provides security on base of domestic and international treads to need for cloud storage system. Each location of cloud server has specific of high cryptosystem.
- In this research paper we are mainly focusing on data privacy and security problem in cloud computing.

3.4 Proposed System

Our main concept in this work is public auditing, that means the integrity of data which has been store on the cloud is checked by TPA. But our work is auditing in cloud and provides high security of private information of data owner. Previous the work which is done in auditing is that there is only two parties one is data owner and another is cloud. In that time auditing has been done by cloud. This concept is known as private auditing. Now the research has been progressed in the area of auditing, what actually has been done is that there comes a new party or third party whose can called as TPA (Third Party Auditor). This TPA and cloud do audit process. This audit process is called public audit. What actually done here is that when user wants to access the cloud, then user need to authenticate first, So by submitting a query in the form of id & password to cloud server and TPA. If a user is already registration in the system then user can be successful login process. If user name and password present in database, then user will login successfully for being valid users or else user receive an error message. In case of new user has to firstly register itself details by filling the registration form and he or she become the active member of system. After successfully login, user will select the file, which user wants to upload on the cloud server. These file will be split into number of blocks. In order to find out the splitting of required file into blocks a file Splitter algorithm is used. In this algorithm, it check if file present or not. If present then file is split in different size based on the file size. For example if the file has 30kb then it will be split into three part 20kb, encryption algorithm. Own system provide to user two option one which are split block encrypted using Data

Encryption standard (DES) algorithm by data owner and another option for block encrypted using Advanced Encryption Standard (AES) algorithm. These algorithms provide confidentiality to the data. It encrypts data blocks of DES algorithm used 56 bits symmetric keys of size 56 bits, and AES algorithm used 128 bits symmetric keys of size 128 bits. After encrypting these blocks, now a hash values are generated, the hashes for each blocks are combined and using BLS digital signature is performed on this process.

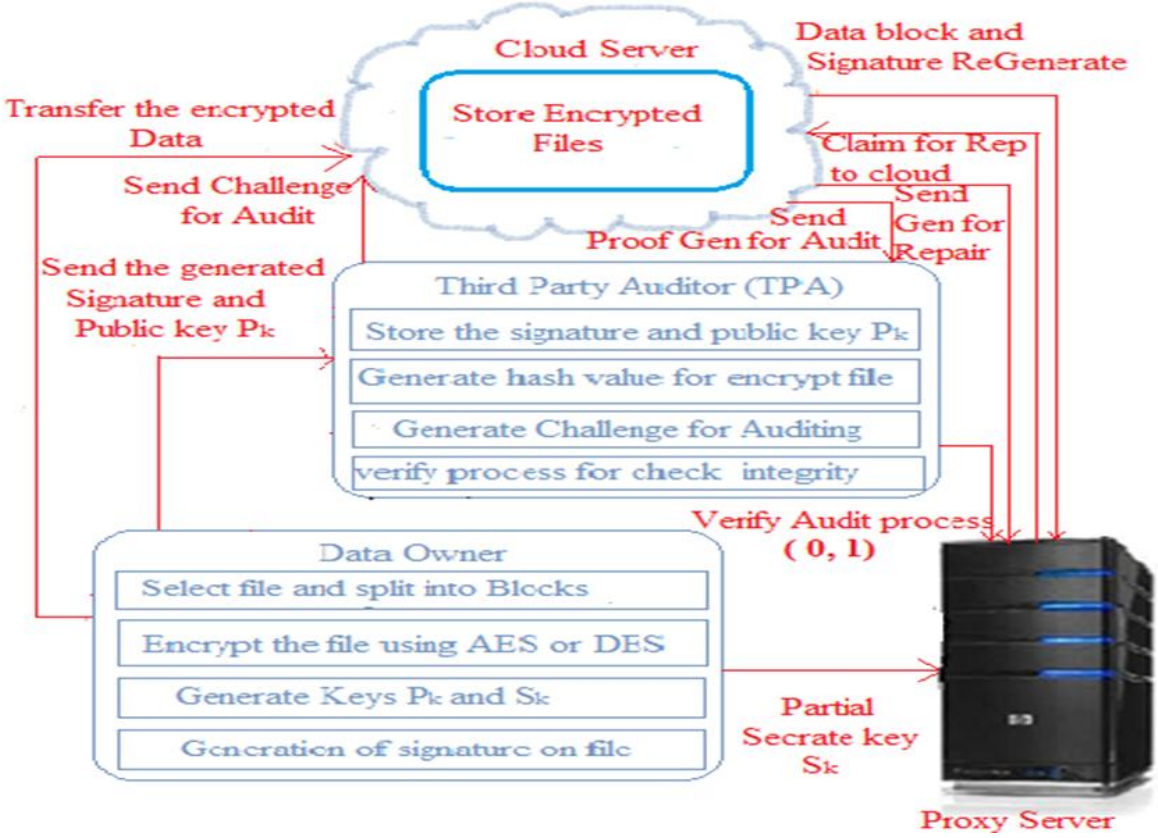

Fig 1: Proposed Data Storage System

4. PROPOSED METHODOLOGY

The main aim of system design is communicate between the use and information system model. The develop input system to measure specification system and procedure for data operation and must be data transaction in a usable form to the computer read and write or print document, The purpose of input system design on controlling the errors, shut down delay, maintain the amount of input need, avoiding the un necessary steps and keeping the process sample.

4.1 Definitions of Our Auditing Scheme

Our system is working on base of public auditing, it consists of three procedures: Setup, Audit and Repair. Each procedure contains are following below.

4.1.1 Setup

This procedure is maintained by data owner for public audit purpose.

a. *KeyGen (Pk, Sk):* - Data owner generate two key one is public key (Pk) and another is secrete key (Sk), and its parameter k as used input. A Public key (Pk) send to TPA by Data Owner.

b. *Delegation (Sk):-* This key is performing to interaction between proxy server and data owner. Data owner send partial secrete key x to proxy server for purpose of behalf of data owner.

c. *Sig and BlockGen (Sk, F)* :- (Φ, Ψ, t) this procedure are used by data owner. A data owner are generate encrypted block set Ψ from original file F, an authenticator set Φ , which is generate the digital signature and a file tag t send to cloud server by data owner.

4.1.2 Public Audit

In this procedure the TPA and cloud server interaction between each other. These takes a random sample blocks from encrypted file and check the data integrity. These check procedures are following below step by step.

a. *Challenge (finfo):- (C*) This procedure is performed by TPA as input of file finfo from original file F and challenge C as output. The TPA sends challenge (info) to cloud server for check data integrity of user.

b. *ProofGen(C, Φ, Ψ) :- (Ƥ)* This procedure run by each cloud server with input challenge C. After TPA send challenge C to cloud server, cloud server generate proof with encrypted blocks set Ψ, authenticator set Φ and challenge C. These contains are combine to make outputs a proof Ƥ. This output proof Ƥ is send by cloud server to TPA for data integrity check.

c. *Verify (P, Pk, C):-* This procedure is performed by TPA, after receive ProofGen Ƥ by cloud server, the TPA store this parameter ProofGen Ƥ, public key Pk, and challenge C as input. The TPA compare these parameter, if compare parameter are same then verification succeed, i.e data integrity are maintained means private data are secure otherwise the information is not secure.

4.1.3 Repair

In Repair procedure, which is work in absence of data owner. This procedure cloud server and proxy server interaction between each other. Proxy server is a semi trusted and it is more powerful then data owner but less powerful to cloud server.it acts on behalf of data owner to regenerate data blocks code on wrong server during the repair procedure and authenticators.

a. *Claim For Rep (finfo) :- (Cr)* this algorithm is performed by proxy server. A proxy send message to cloud server to Claim for repair Cr or regenerate the data block.

b. *Gen For Rep(Cr, Φ, ψ) :-* (BA) This procedure are run by cloud server, after receive Claim For Rep(finfo) Cr by proxy server then cloud server start the procedure to repair the wrong server and finally output generate the set of block data and authenticator is BA with the help of two input Φ and Ψ.

c. *Block and SigRegGen (Cr, BA):-* (Φ, Ψ, ⊥) this procedure are performed by proxy server. After receive BA from cloud server. It implement this algorithm (Block and SigRegGen) with claim Cr and response BA from each cloud server as form input, and it makes output new encrypted data blocks set Ψ'and authenticator set Φ', if this procedure are successful then it generate output ⊥.

4.2 Proposed Algorithm

Implementation of our project is the stage to convert to theoretical design into a working system. It designs to achieving a successful new system from process of various critical stages. And it is giving the user, confidence that the new system will work and be effective.

The implementation stage design the various area investigations of the existing system, careful planning and constraints on designing of Algorithm to achieve changeover and evaluation of changeover methods. Our system is working on this Algorithm.

1. Select a file & split into blocks
2. Use file Splitter algorithm for file split into blocks
3. Encrypt the data block of file
4. Let n = number
5. Switch (n)
6. {
7. Case: 1
8. {
9. Use DES Algorithm for block encrypted
10. }
11. Case: 2
12. {
13. Use AES Algorithm for block encrypted
14. }
15. Default:
16. {
17. You choose either 1 or 2
18. }
19. }
20. Generate hash value for block of file using BLS Signature Algorithm.
21. Concatenation of all the blocks of file.
22. Generate keys Pk, Sk and Signature.
23. Send partial secrete key Sk to proxy server.
24. Send public key Pk and signature to TPA.
25. TPA receive public key Pk and signature send by user
26. Generate hash values for each blocks of file
27. Concatenation of all the hash value
28. Generate signature by TPA
29. TPA send challenge for audit to cloud
30. Receive the proof generate required data send by user
31. In case data owner absent
32. Proxy server randomly contacts to cloud server to claim for repair blocks
33. After receive generate repair block by cloud server
34. Proxy will execute batch verification for the received blocks
35. If verification is fail. Then
36. {
37. server connected to malicious for repair, proxy aborts the reparation
38. }
39. Else {
40. continuous to generate new coded blocks and authentications
41. }
42. End if
43. End.

5. RESULT ANALYSIS

This proposed system provides high security to user information in comparison of existing system. We evaluate the efficiency of our multi-cryptosystem based privacy-preserving public Auditing for regenerating-code-based cloud storage system is very high. which method design is perfectly lightweight for the data owner to execute. Because our privacy-preservation public audit method implements only once time during the whole life of a user's file. Our system

has used two cryptosystem DES and AES. These are following strength given below.

5.1 Data Encryption Standard (DES)

Data Encryption Standard Algorithm is use in proposed system with a key length of 56 – bits.

Strength of DES

a. It means, there are 256 possible keys, we can be used.

b. The existing system is used to mask the coding coefficients technique for encoding process. While ours choose DES cryptographic technique. If attacker wants to break DES cryptographic system, then would require more than 1000 years from a single computer. It seems that attack on this proposed system is impractical. Hence numerically comparing them, we can see that our privacy preserve method is more securing then existing system.

5.2 Advanced Encryption Standard (AES)

Data Encryption Standard Algorithm is use in proposed system with a key length of 128 – bits.

Strength of AES:

a. With 128 bit: 2128 = 3.4x 1038 possible keys

b. A PC that tries 255 keys per second needs 149.000 billion years to break AES.

5.3 Comparison

S no	Characteristics	Proposed Encryption Algorithm		Existing Encryption Algorithm
		DES Algorithm	**AES Algorithm**	**Homomophic Algorithm**
1	Keys Used	Same key used for Encryption & Decryption	Same Key used for Encryption & Decryption	Only Private Key used Encryption & decryption
2	Security applied	Both side (User and Cloud)	Both side(User and Cloud)	Cloud Provider only
3	Key Length	56-bit	128-bit	Variable(one or two)
4	Block Size	64-bit (Block level)	128-bit(Block level)	Bit level
5	Security Rate	Good	Excellent	Not enough
6	Encryption & Decryption Capacity level	Encrypt & Decrypt to full disk, database, file, distributed storage and row and column level	Encrypt & Decrypt to full disk, database, file distributed storage and row and column level	It is used to perform complex mathematical operation on encrypt data without compromising encrypt

Table 1 Comparison between Cryptosystem Strength

This proposed system provides two cryptosystem algorithms in specification data storage system. Cloud service provider is store encrypted data in form of two techniques (DES or AES), hence attacker can be confuse whose code are encrypted DES and AES. So it is not easily finding out the encrypted code. Therefore To measure the strength of security in compare of proposed system is more than existing system.

Above show that table 1 compare between propose cryptographic algorithm and Existing cryptographic. So we find out result is proposed system more secure than existing system. This system measure security strength by all parameter, then find that proposed system is very secure data store in cloud to compare to existing system.

6. CONCLUSION

We have proposed system to provide end user to different level of data security. The main issue of analysis of cloud server and related to data storage security in cloud storage system. Some security of specially data integrity and privacy are key generate issue. A user store data in cloud as publically and he/she doesn't knows his data store exact location and which cryptographic are used. It provides a secure and efficient privacy preserving public audit scheme for regenerating-code-based cloud storage system by help of proxy server. In this scheme TPA does not retrieving the data copy, hence privacy is preserved. The file is split into blocks and the stored in the encrypted format with help of either AES or DES algorithm in the cloud server, thus secure the protection of data. The data integrity verifies by TPA, it verifying both signature on demand or periodic audit scheme. Proxy server and cloud server are regenerating the data block and authentication at absent of user. Proxy server works as behalf of user. To better provide data security to design our authentication based on the BLS signature. Hence this system is attempt made to overcome the limitations of the existing auditing scheme. Implementation of project is the stage to convert to theoretical design into a working system. It is giving the user, confidence that the new system will work and be effective.

In future work, we would like to perform data share multi user and data dynamic operation such as updating, deletion and insertion of data.

7. ACKNOWLEDGMENTS

I owe an enormous debt of gratitude to my thesis supervisor, Prof. Rajit Nair, for guiding and inspiring me from the beginning through the end of this thesis with his intellectual advices and insightful suggestions. I truly appreciate and value his consistent feedback on my progress, which was always constructive and encouraging, and ultimately drove me to the right direction. I wish to thank my father Mr. Rajaram Prasad chaursia, my mother, Brother Niku Kumar all my family members and my son Adhayan prakash for their unwavering faith and belief in me throughout my life. I would have never made it this far without their support that was beside me in every step of the way.

8. REFERENCES

[1] Jian Liu, Kun Hun, Hong Rong, H.Wang and M. Xian, "Privacy-Preserving public auditing for regenerating-code-based cloud storage", IEEE Transaction on information forensics and security, vol. 10, no.7, JULY 2015

[2] Swapnali More, Sangita Chaudhari, "Third Party Public Auditing schemes for Storage" 7th International Conference on Computing and Virtualization 2016, Future Generation Computer Systems, Elsevier.

[3] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[4] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Compute., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[6] Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., & Zeghlache, D. (2011). Challenges for cloud networking security. In Mobile Networks and Management (pp. 298-313). Springer Berlin Heidelberg.

[7] Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010 (pp. 1-7). IEEE.

[8] S Ezhil Arasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277, 3878, 2013.

[9] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as the 5th Utility", Future Generation Computer Systems, Elsevier, Vol. 25, pp. 599-616, 2009.

[10] Mell, Peter, and Tim Grance. The NIST definition of cloud computing. (2011).