Ensuring Privacy and Integrity of User's Data on Public Cloud

Vitthal Sadashiv Gutte, Kamatchi Iyer

Abstract: ***in the cloud store the data and use it from anywhere in the world but the users are worried of the data stored on the cloud in aspect of data integrity and validation of data. Therefore we are using Third Party Auditor (TPA) to ensure data integrity for ensuring data correctness on cloud. There are many auditing schemes existing but they have limitation so that we come up with a new approach of auditing. In this paper we have implemented a new scheme which efficient in performance over the cloud. It consists with two key one with users private and other with user's public key. The user key has created a hash value from all the data with encoding framework. TPA performs the validation of data throughout any user's action over the cloud. TPA generate the own signature and validate with users signature and keep the log of data all the time. It matches the both signature for data correctness .Validation of data shows the movements on users demand. The server keeps the all data watch over the performing action by users and TPA. The main objective is to show the correctness of data on cloud, maintain the integrity of data and provide a secure channel for privacy over the cloud usage. We have frame architecture to minimize the cost of cloud with TPA where minimum use of data on the TPA side. The system supports to batch auditing process and dynamic updating in usage***

Index Terms: Cloud Computing, Third party auditor (TPA), Batch Processing, Signature.

I. INTRODUCTION

Usage of cloud is growing every day. The Cloud usage service helps the users to feel free from the burden of storage data at different physical location. Just store at one place and use it from worldwide. Even though this is provided by the cloud but it's under the attack from different attacker's .This data should be free from attack and integrity should be maintained throughout the procedure [9].

In the response to the users demand the auditing perform though different angles .First the auditing framework efficiency for every operation throughout the network.

Secondly cost effectiveness of that auditing system with good efficiency. At last the parameters used for the procedure which effects on the complexity calculations over the all operations [3].

Revised Manuscript Received on July 05, 2019

Vitthal Sadashiv Gutte, Research scholar at Computer science engineering, Amity School of Engineering and Technology, Amity University Mumbai. Pin code: 410206, India.

Dr. Kamatchi Iyer, Professor at Computer science engineering, Amity School of Engineering and Technology, Amity University Mumbai. Pin code: 410206, India.

.

At a place where different type of data security is provide. The data is split into different parts where the data blocks are stored at different places. The every data has to maintain the integrity of it which should be calculated on the auditing process. In present schemes where the data integrity is checked but most of the work with the duplicate copy stored at some other place and check for integrity in auditing.

Some systems [10] are available for auditing but it does not support the dynamic auditing process in the cloud .There are several schemes evolved to support the dynamic as well. The systems use the different format to show the out.

In a procedure of existing systems most of the scheme not able to track leaked data. They are not able to provide security against the unfamiliar cloud provider. This leads into problems in the cloud .It grows the complications in the cloud architecture [11].

Homomorphism authentications (HARS) scheme is different from the ring structure method which was convolution [6]. Ring structure has a feature which preserve the identity of the users .It does not prove the data during critical situations and not able to prove data freshness.

In this paper we have worked on different privacy issues which were not solved with the previous work. We have implemented a system with the use of signature where the complexity gets increases of algorithm with the current system time in the algorithm. We have used the modified RSA algorithm for the signature creation with MD5. Our TPA system is different than the other where our TPA creates his own signature and compare with the existing signature in database.

It works on the batch auditing procedure whenever users want to check the integrity or correctness of data. Our approach shows that we have minimized the cost of data on cloud as we are not keeping duplicate copy on TPA side for comparison. Our system is more efficient in communication as we are using TPA signature with the use of foreign key of users. Our TPA is completely different from existing system

II. LITERATURE SURVEY

[1] In this paper Auditing of data is performed which support the dynamic operations for the computing digital signature. It preserves the structure of that data with the use of index value in hash tables. The different in this paper the author has divided into different model

to generate significant results.

[2] The author has work on the identity privacy over the cloud usage data. They have kept the updated data that means they have maintained the fresh data. They have used Homomorphic Authenticable ring signature (HARS) scheme to preserve the data of user. The author also used the overlay tree concept to keep the data freshness. They have used TPA for the auditing purpose. They have worked on trustworthy CSP cloud service provider without disclosing identity in group.

[3] The author work on the auditing system. He has taken the different entity for the consideration .TPA has download, upload functions. The author talks about hackers in the concept of integrity maintaining. The method Dynamic privacy preserving but author failed to explain any new approach to solve the problem .Author has proposed cloud security algorithm (CSA) but failed to propose the execution of algorithm with efficient results.

[4] The paper talks about the data security and integrity as a main focused area. The author concern about data owner's authority over the cloud. The paper talks about the dynamic approach over the data integrity. The method explained in paper about the elliptic curve cryptography differ Hellman signature method is used with improved distributed hash table for the data structure. The author has explained with the minimum storage cost but failed to give the procedure is dynamic or not. Author unable to explain about the batch auditing .The results shows are not as per the claimed data.

In table 1 we have studied about different approaches which were worked in this area. This study helps to comparison between different studies.

Table 1: Comparative study

Title Of Work	Methodology	Public Auditing	Privacy Preserve	Data Integrity	Confidential users data	Communication Cost minimize
PPA-SCS [13]	HLA with BLS	Yes	Yes	Yes	No	No
PPPA –CUHMAC [7]	HAMC	Yes	Yes	Yes	No	No
PPPA-DSSC [8]	HLA in RM	Yes	Yes	Yes	No	No
SEPPPA-SCS [10]	HLA in BLS	Yes	Yes	Yes	No	No
TSD-SSCC [12]	Homomorphic Tokens	Yes	Yes	Yes	No	No

III. EXISTING SYSTEM

In most of the existing system different mythologies have been used on of the existing methodology [5] which is mainly focuses on security issues of cloud data storage during all system operations. The methodology has three different entities involved as follows in figure no 1.

- Cloud user It consist all type of users
- Third Party Auditor (TPA)
- Cloud server.

Once the data owner authenticates over cloud server, the data owner selects the file to upload in cloud, after uploading file it gets split into blocks. The blocks are gets encrypted using AES algorithm followed by generating message digest using Secure Hash Algorithm (SHA-2). A copy of encrypted file is transferred to cloud for storage purpose. Later the message digest is sent to TPA. TPA uses this digest to check the integrity of data stored in the cloud server storage. Since metadata is sent to TPA, TPA will not get enough information about users actual data thus achieves user's data privacy.

In this system TPA performs data auditing on demand by the client. On receiving the auditing request from cloud user or data owner, the TPA challenges cloud server to send the encrypted data of files that are stored in cloud. After getting the encrypted data from cloud server the TPA follows the same process performed by data owner such as generating message digest for encrypted blocks of data using SHA-2 algorithm

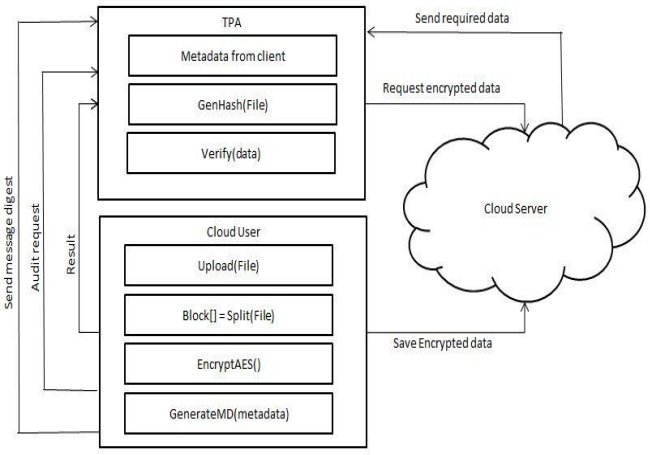

Fig. 1: Auditing approach [5]

Later in verification process, it compares the newly generated message digest value with the earlier message digest sent by client. If both the values are matched then it indicates that the integrity of data is maintained. If there exists a mismatch, indicates that data is altered and integrity is not maintained. Finally the TPA will send auditing results to the data owner indicating the status of file.

The cloud server is used to store the encrypted data of

files. When it receives request from the TPA, the cloud server will send required encrypted blocks of data to TPA. In the proposed scheme cloud users can upload files to cloud server and can rely on TPA to check the integrity of data stored in cloud server.
In this system synchronous key encryption is used that is same key is used for encryption as well as decryption which is a huge security threat.

IV. PROPOSED ARCHITECTURE

The cloud user: needs to store large number of data files on cloud serve, the cloud server: it is managed by cloud service provider, who is responsible for providing data storage service and has significant storage space and computation resources; the third-party auditor: has the expertise and capabilities which user does not have and on users request has access to cloud storage service. The data is no longer in local possession of the user, so it is very important to ensure that the data is correctly stored and maintained on cloud servers. The user may delegate the task of checking data integrity to a third party auditor (TPA), this will save user resources and computation time.
In this architecture we have proposed a scheme which works more efficiently with the flexibility maintained on distributed scheme. This also support for dynamic data approach to for the correctness of users data over the cloud based system. We are also work on the correcting code which relies on erasure code in file storage. This helps to provide data redundancies and guarantee the data dependability in complete performance. Our approach helps to build up repository system to facilitate integration of data as well sharing data across the cloud. Even this perform we have preserved the confidentiality over the cloud

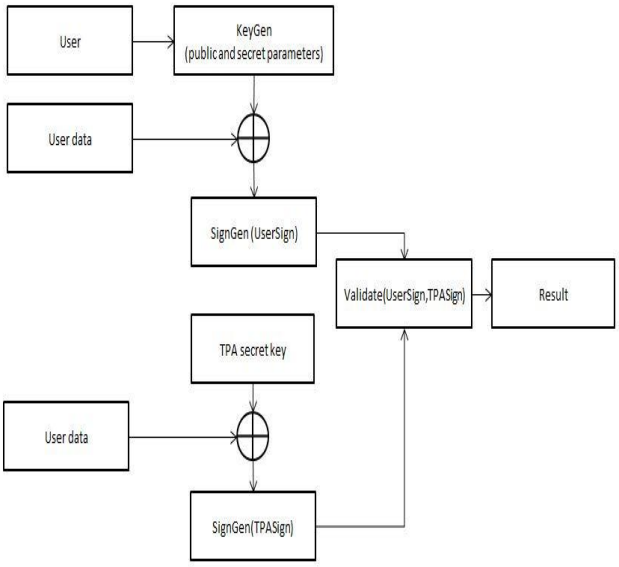

Fig. 2: Proposed auditing scheme

A public auditing scheme consists of three algorithms (KeyGen, SigGen, VerifyProof). The algorithm for KeyGen is used to generate a key which will run by the different user to setup scheme on cloud usage.. SigGen is generated two times first while uploading data by user and secondly to verify data on TPA side by TPA, which may consist of users key and data. The operation performs the VerifyProof by the TPA for the auditing purpose over the system. In a system for public auditing process it consist the two different phases for execution over the cloud.

Setup phase: In this phase a user's initialization process occurs where public and secrete parameters of system get execute by the KeyGen. This will happened for the creation of keys. The KeyGen generates two types one is secrete key which is public key Pukey and other is private key which is Prkey, and user then generates the digital signature using SigGen. SigGen takes Prkey and File F to generate digital signature. The user then stores the data file F and the digital signature of that data at the cloud server.

Audit phase: The TPA issues the auditing information in the message to make sure that the cloud server has the retained file in a proper format. The method of TPA will derive a response message from the function of data which is already stored there. The execution process with the VrifyProof. VrifyProof generates another digital signature using the current data of the file and users Pu Key which is public key. The next procedure is TPA will verify both the signature to evaluation of the data integrity on the cloud. The TPA is stateless that the TPA does not need to maintain the update state between the audits. This is much desirable property of public audit scheme, but the TPA follow the execution process every time whenever needed.

Implementation of TPA

The work of Third Party Auditing is to Audit various files in the cloud and give the report whether the files in the cloud are secured. In this project TPA can audit many files in the cloud at a time. But the same file of a single user will also be audited by a TPA at a time. Different files of various users' will be sent TPA in the same time. At the same time in this project TPA will not locally download the file for Auditing. TPA can also audit many files at a same time which cause less time for auditing many files by TPA. TPA uses file and user's public key to audit and send report to the particular user.

V. RESEARCH METHODOLOGY

In our approach the auditor has a capability to audit data with greater efficiency. The auditor has a read only authority while performing operations. This support dynamic approach while performing operations. It checks the correctness of user's data over the cloud applied system. This is trustworthy

for the system. This also supports the batch auditing.

In our approach we are creating signature with user's data. We are also including the current system time of that machine for generating a signature. We have used RSA with MD5 for creating a signature and store on the cloud. We have added additional parameter while generating signature that is current system time. This helps to create a signature with more random possibility. Even thousand users with same data comes then also everyone will have different signature because the system time of every machine will be different at the time of save. The system time in millisecond so mostly time of saving this must be different for every individual.

Our goal is to minimize the storage cost and keep the data freshness through the operations in the cloud system. To achieve this we have implemented an effective system in our proposed architecture. In minimum communication TPA generate his own digital signature with decryption of data of users. The TPA has only read-only capabilities so that it will not able to change the data in our cloud database. It takes public key of user and enter in data base for the decryption of data. After this it will generate his own signature with all attribute of users and finally generate a signature

In our approach the communication efficiency increases as we are not burden with data copy storage. We have found that data correctness of users is more confidential as we are not sharing private key while decryption .The storage cost is minimum because we are not keeping any data copy to TPA. This all-time generate his own signature and perform the validation function. The user has its own signature while performing save operation .The log of authorize users is maintained .the signature also changes as an authorized user change the data. This helps to keep the freshness of data continuous in orations. As an intruder comes and change the data then TPA will have different signature than the users own signature. The system performs in batch processing so that large data operations perform in quick action. This system also support for the response time for user on cloud without any burden on data storage for different attacks

VI. ALGORITHM

Algorithm for the uploading file on the cloud service in our system.

1) Algorithm for File Upload

INPUT: i) File
ii) Private Key (Uploader's)

OUTPUT: i) Digital Signature

```
1) //Input File
   Upload(File)
2) //Read File content
   Byte[] filedata = ReadFile(File)
3) //Get Private Key of user
   Byte[] pr_key = getPrivateKey(EmailID)
4) //Generate Digital Signature
   Byte[] = GenerateDS(pr_key,filedata)
5) //Save file
   Save(File)
```

Algorithm for the verify the approach in on our System with efficient approach. The output consists of signature and also the result of confidentiality.

2) Algorithm of File Verify

INPUT: i) File
ii) Public Key
iii) U_DS

OUTPUT: i) Digital Signature
ii) Confidentiality result

```
1)  //Get Public Key of user
   Byte[] pu_key = getPublicKey(EmailID)
2) //Read File content
   Byte[] filedata = ReadFile(File)
3) //Generate Digital Signature
   Byte[] TPA_DS = GenerateDS(pu_key,filedata)
4) //Validate
   varified = match(U_DS,TPA_DS)
5) if (verified)
     Print.out("Verified")
   Else
     Print.out("Data violated")
```

VII. MATHEMATICAL MODEL

The protocol consists of four algorithms; KeyGen is run by the client and generate user side signature and store it over cloud along with file, SigGen is run by the client as well as TPA to generate verification result.

VerifySign which is run by the TPA. TPA verifies both the signatures and the proof of correctness of data.

ExecUpdate is run by user while updating file to regenerate the signature for updated file

KeyGen() → (PuKey, PrKey). Run by the client. Creates a public and private key pair.

SigGen(PrKey, F) → (φ, sign(H(R))). Run by client. Creates a set of signatures φ = {Uσi} for file F to store over cloud.

SigGen(PuKey, F) → (φ, sign(H(R))). Run by TPA. Creates a set of signatures φ = {Tσi} for file F to verify file integrity.

VerifySign(Uσi, Tσi) → {T RUE, F ALSE}. Run by TPA. Verifies the proof, using the user's digital signature and TPA digital signature. Returns true or false.

ExecuteUpdate(F, φ, update) → (F' , φ' , update). Run by the client. Performs the update on the file, and returns the new file and signature.

VIII. RESULT ANALYSIS

To achieve constant bandwidth, we took files ranging from 100KB to 1000KB. The figure 4

represents the time taken by TPA to audit the files ranging from 100KB to 1000KB. In our observation, comparing our proposed system with NDADPDC framework [5], we find that our system will also take constant time to audit the files of different file

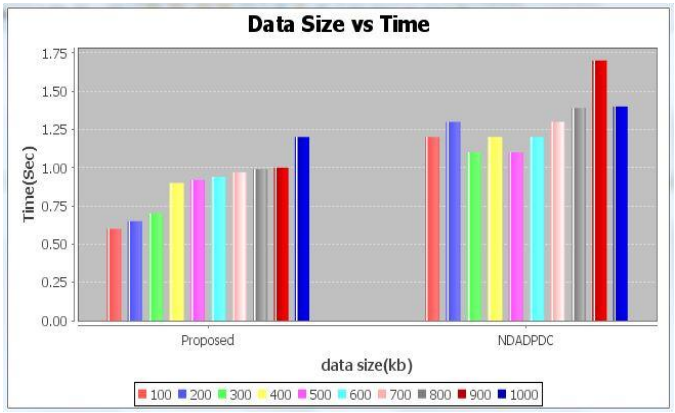

Fig.4: Data size vs. Time

Figure 5 depicts the simulation graph which includes number of clients on y axis and average auditing time taken for each task on x axis we have compared the time with EASDSC[3] framework by taking same number of clients, as per figure 5 proposed system takes less time to audit.

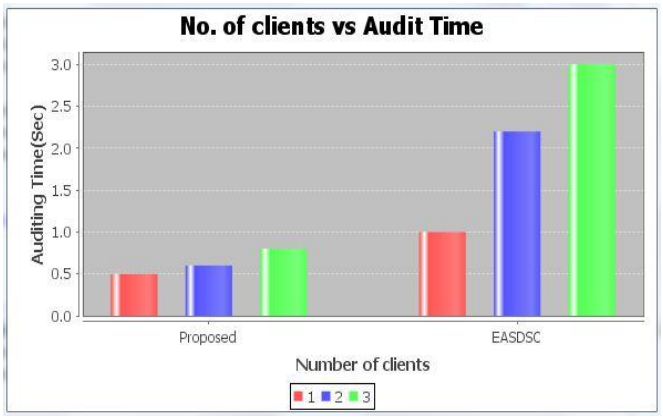

Fig 5: No. of Clients Vs Audit time

Figure 6 shows the performance time required to upload, audit and download for variable file size

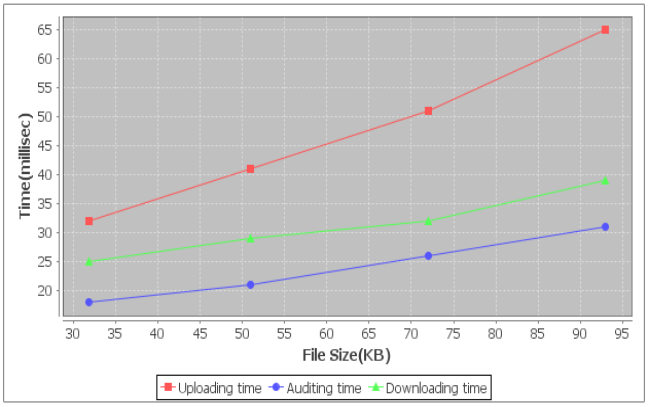

Fig. 6: Performance time

Figure 7 shows the comparison between RSA and DES algorithm. We used RSA to generate key pair in implementation. Comparatively RSA takes less time to generate key pair

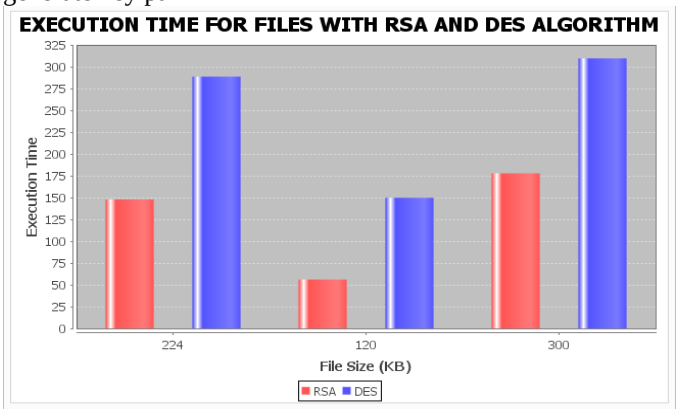

Fig 7: Execution time with RSA & DES

IX. CONCLUSION

This proposed system utilize the asynchronous keys to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user , but also alleviates the users' fear of their outsourced data leakage. In a process of cloud operations on data of an every user is kept stored with all security concern, User can confirm the integrity with the TPA with efficient approach over cloud. In future we can also expand this auditing protocol for various types of data format as in this project the auditing is performed on document only, in future work the auditing may be perform not only on data and image but also on video, pdf etc.

REFERENCES

1. K. Swathy , dr. N. Velvizhi "Public audit on dynamic data preserving user identity and data freshness" sixth international conference on advanced computing (icoac), 2014.
2. Tina esther trueman1 p.narayanasamy2 "Ensuring privacy and data freshness for public auditing of shared data in cloud" ieee international conference on cloud computing in emerging markets 2015.
3. Jayashree agarkhed ,ashalatha r. "An efficient auditing scheme for data storage security in cloud" international conference on circuits power and computing technologies [iccpct] , 2017 .
4. Esther daniel "A cost effective dynamic auditing scheme for outsourced data storage in cloud environment" ieee international conference on innovations in green energy and healthcare technologies (icigeht'17) 2017.
5. Shivarajkumar hiremath sanjeev kunte "A novel data auditing approach to achieve data privacy and data integrity in cloud computing" international conference on electrical, electronics, communication, computer and optimization techniques (iceeccot) 2017.
6. Bboyang wang, baochun li, Hui li " Oruta: privacy-preserving public auditing for shared data in the cloud", ieee transactions
7. On cloud computing, **page** 43 - 56 ieee transactions on cloud computing (volume: 2, issue: 1 , jan.-march 2014).
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, volume 2, issue 1, pp. 149-152, march 2013.
9. Wang, c., wang "Privacy-preserving public auditing for data storage security in cloud computing" infocom, 2010 proceedings ieee, 2010.
10. Boyang wang et al. "Panda: public auditing for shared data with efficient user revocation in the cloud" ieee transactions on services computing (**page:** 92 – 106

volume: 8 , issue: 1 , jan.-feb. 2015)
11. Solomon guadie worku, chunxiang "Secure and efficient privacy-preserving public auditing scheme for cloud storage". Computers and electrical engineering, pages 1703-1713, volume 40 issue 5, july, 2014.
12. Cong wang et al. "Privacy preserving public auditing for data storage security in cloud computing" 2010 Prceeding IEEE INFOCOM doi**:** 10.1109/infcom.2010.5462173 , 06 may 2010.
13. Cong wang et al. "Toward secure and dependable storage services in cloud computing" IEEE Transaction on services computing. Page 220-232, volume 5, issue 2, april-june 2012.
14. cong wang, qian wang "privacy-preserving public auditing for secure cloud storage" ieee transactions on computers (**page:** 362 - 375 volume: 62 , issue: 2 , feb. 2013) **doi:** 10.1109/tc.2011.245.

AUTHORS PROFILE

Vitthal Sadashiv Gutte,
Research scholar at Computer science engineering, Amity School of Engineering and Technology, Amity University Mumbai. Pin code: 410206, India.

.

Dr. Kamatchi Iyer
Professor at Computer science engineering, Amity School of Engineering and Technology, Amity University Mumbai. Pin code: 410206, India.