ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Privacy Preserving Public Auditing for Cloud Storage

Nandini P. Wasnik, Prof .Mahip M.Bartere

M.E. Final Year CSE, GHRCEM, Amravati, India

Assistant Professor, Department of CSE, GHRCEM, Amravati, India

ABSTRACT: As cloud provide facility for the user to store their data easily as well as good quality of cloud applications which is need not install in any local hardware and software system. such a service is also gives users control of their outsourced data, which also provides control to the security problems regarding the correctness of the data storage in the cloud. The important roal of cloud computing the data protection, secure and the process data stored under the property of users. Data which is stored at the server how that cloud users will get the confirmation about data which is to be stored. That’s why cloud storage should have some technique and mechanism which will specify correctness of data storage and integrity of data stored on cloud. For this reasons the users can refer to a third-party auditor (TPA) which is to check the integrity of outsourced data ,TPA should be able to efficiently audit the data storage on cloud . To proposed an effective and also secure TPA auditing process. In this paper, we propose system for a cloud storage which is the secure and supporting privacy-preserving public auditing. The proposed system perform for multiple users auditing process simultaneously and efficiently.

KEYWORDS: Data storage, privacy preserving, public audit ability, cloud computing, batch verification

I. INTRODUCTION

In the history of IT, cloud computing has brought unprecedented benefits to the computing world. It has made it possible to have a different computing model that does not suffer with scarcity of resources. Cloud computing enables to share computing resources without the need for investment in pay as you use fashion. Cloud service providers such as Microsoft, Oracle, Amazon, Google etc. are able to provide huge clouds which are nothing but computing resources that are provided on demand through Internet(1).The way on that IT infrastructure has been used; is changing with the emergence of cloud computing. One important part of cloud computing is that data which is stored in a centralized server is linked to data centre of cloud . The storage and other services provided by cloud can be utilized by individuals and organizations alike without the need for capital investment. For organizations and individuals cloud provides very useful advantages as they are relieved from storage management, investment, and maintenance. (2).

Moreover, it help users to evaluate the risk of their subscribed services of cloud data, the audit result from TPA would also be important for the cloud service providers to improve their cloud-based service platform, and even serve for independent arbitration purposes (5). In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud. Recently, the notion of public audit ability has been proposed in the context of ensuring remotely stored data integrity under different system and security models . Public auditability allows an external party, in addition to the user himself, to verify the correctness of stored data. However, most of these schemes do not consider the privacy protection of users’ data against external auditors. Indeed, they may potentially leak user’s data to external auditors, this drawback greatly affects the security in cloud computing. For the purpose of protecting data privacy, the users, who own the data , rely on TPA just for the storage security of their data, toward their data security(6). As the individual auditing of these growing tasks can be tedious, a natural demand is then how to enable the TPA to efficiently perform multiple auditing tasks in a batch manner, i.e., simultaneously.To address such type of problems, the technique of public key-based homomorphic linear authenticator used , which enables TPA to perform the auditing task of data without demanding the local copy and thus reduces the communication cost and computation overheads.

DOI: 10.15680/ijircce.2015.0306068

By merging the HLA with random masking, the used protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server (CS) during the efficient auditing process.

II. PROPOSED SYSTEM

The proposed system contain following three entities, as show in Fig. 1: cloud user (U), which contain the amount of data files which are stored in the cloud;
cloud server (CS), managed by the cloud service provider (CSP) for providing storage service, storage space as well as computation resources ;

third party auditor (TPA), who has the capabilities and intelligient that cloud users does not have and TPA trustfull for assessing the reliability of cloud storage upon request of the user . Users can depend on CS for cloud data storage and maintenance, also dynamically interact with the CS for accessing and update the data stored for purpose of various application . To save the computation resource as well as the online limitations ,the users of cloud may resort to TPA for ensuring their outsourced data storage uniquess, which to keep their data private from TPA. It is most importance to enable public auditing service for cloud data storage, so that users resort to an third party auditor (TPA) which is not dependent to audit the outsourced data when ever needed. The TPA, which make it a much more easier and efficient way for the users to ensure their storage correctness in the cloud. Moreover, for evaluate the risk of the cloud user the audit analysis result from TPA would also be important for the cloud service providers to improve the cloud based service platform, and even serve for independent negotiation purposes.

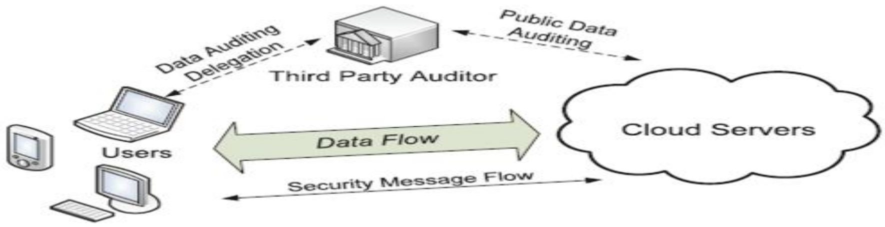


Fig:-Architecture of cloud storage provider

1. System Modules

1. System Module
2. Privacy-Preserving Public Auditing Module
3. Batch Auditing Module
4. Data Dynamics Module

1.1 System Module

User: users, who have data to be put in the cloud and also for cloud data computation, which is both individual consumers and organizations.
Cloud Service Provider (CSP): CSP, who has resources capabilities and expertise in building organised distributed cloud storage servers, and operates Cloud Computing systems.
Third Party Auditor (TPA): is trusted for accessing and evalute risk of cloud storage services on behalf of the users upon request.

1.2 Privacy-Preserving Public Auditing Module

Overview to achieve privacy-preserving public auditing, the propose system has to uniquely combine the homomorphic authenticator with random mask technique. In this protocol, the linear combination of sampled block is masked with randomness generated by a pseudo random function (PRF).
The proposed system consist of two phases:

- Setup Phase
- Audit Phase

1.3 Batch Auditing Module

In batch auditing module not only allows TPA to perform the multiple auditing tasks of different user simultaneously, but also it decreases the computation cost on the TPA side.

1.4 Data Dynamics Module

Support data dynamics, including block level operations of modification, deletion and insertion, this technique in our proposed system design to achieve privacy-preserving public risk auditing with support of data dynamics.

2. Proposed system framework

A public auditing scheme consists of four algorithms
Key Gen is a key generation algorithm which is run by the user.
Sig Gen is used by the cloud user to generate verification metadata, and also other related information that will be used for auditing purpose.
Gen Proof is run by the cloud server to generate a proof of data storage .
Verify Proof is run by the TPA to audit the proof from the cloud server.
The public auditing system consists of two phases, Setup and Audit:
• **Setup:** The cloud user firstly analysis the public and secret parameters of the proposed system by executing KeyGen, and then again pre-processes the data file F by using Sig Gen which generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server.

• **Audit:** The TPA issues an audit message to the cloud server which make confirm that the cloud server has retained the data file F properly at the time of the audit By executing GenProof ,the cloud server will derive a response message from a function of the data stored file F and its verification metadata. Via Verify Proof the TPA verify verification proof .

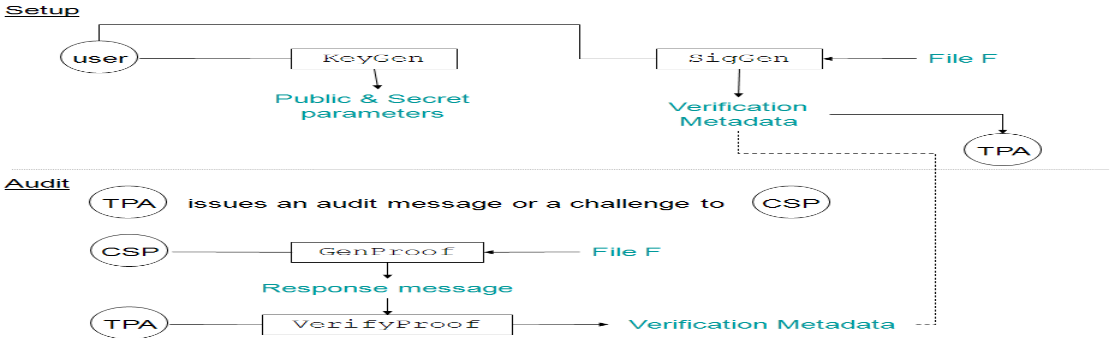
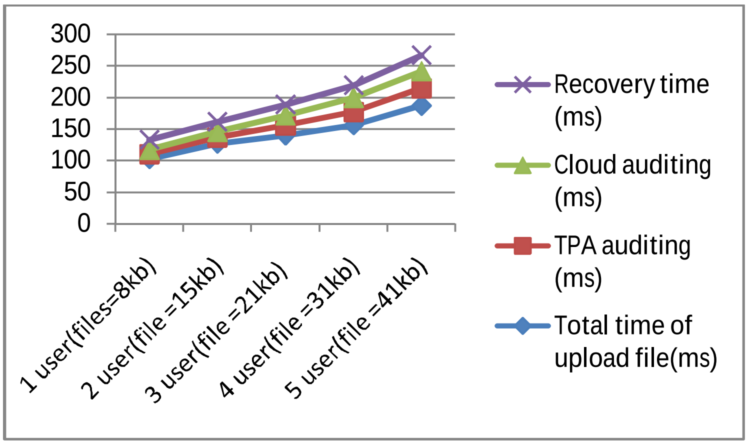


Fig:- Working of two phases

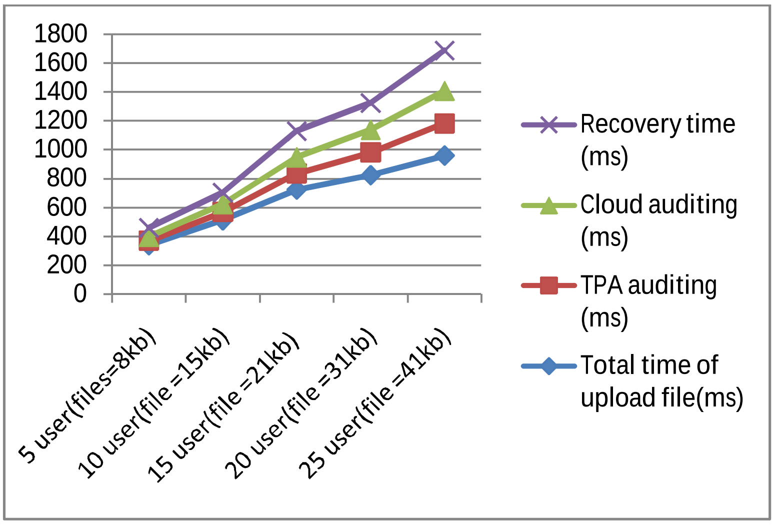
III. EXPERIMENTAL RESULT ANALYSIS

Microsoft Azure cloud is used to store and retrieve data. The cost of privacy preserving protocol is evaluated with many experiments. Then we focused on batch processing efficiency as well. The quantification of cost enabled us to assess the performance of the protocols implemented in this analysis. Suppose there are c random blocks specified in the challenge message chal during the Audit phase. Under this type of setting, we identify the cost which is introduced by the privacy preserving auditing in the terms of server computation, auditor computation as well as communication overhead. Since the difference for choices on s has been discussed previously, in the following privacy-preserving cost analysis we only give the atomic operation analysis for the case for simplicity. The analysis for the case of follows similarly and is thus omitted. On the side of server , the generated response includes a aggregated authenticator.
As shown7.1 perform system analysis for individual auditing by taking five no of user along with their different file size, total time of upload file, auditing time and also its recovery time.



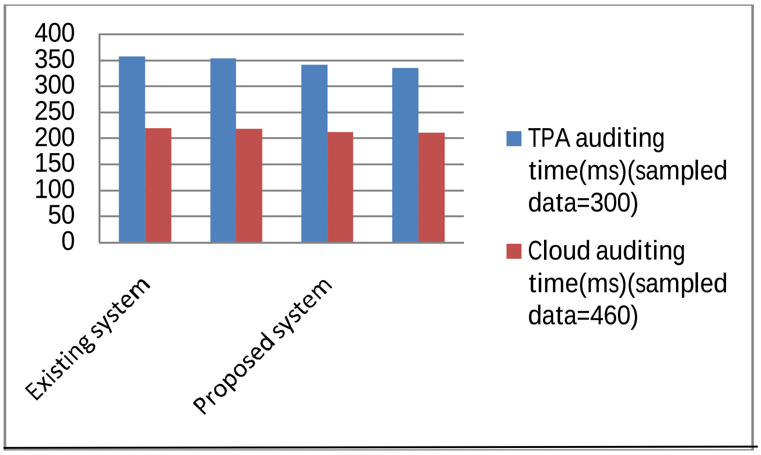
In individual auditing the user can upload different size of data, as here we take five different types of user with their different file size TPA auditing time and cloud auditing time is calculated as compare to both auditing time the recovery time taken is less and it executed very fast.

As shown 7.2 perform analysis for multiple user that is batch auditing task by taking multiple user including total time of file upload, auditing time and also recovery time.



As shown 7.3 perform analysis of existing system and proposed system comparison as from existing system the sampled block of data generated during auditing process are more than proposed system and thus proposed system audit process of data fast than existing system. The sampling block of data generated by response of server and it get vary according to the size of the data upload from this it notice that the sampling of data is increases its recovery time also get require more time.

DOI: 10.15680/ijircce.2015.0306068



IV. CONCLUSIONS

Proposed system introduced a data storage security in cloud computing. Proposed system uses the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content which is stored on the cloud server during the efficient auditing process, which not only reduces the burden of cloud user from the tedious and possibly expensive auditing task. The process as data user can check the integrity of their data stored in cloud server using TPA which can be done in efficient manner. If any changes find out in data by the TPA, TPA will immediately intimate to the owner of the file and so security and data integrity is secured properly. The proposed system also introduces the privacy-preserving public auditing protocol into a many user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

REFERENCES

[1] T. Schwarz and E.L. Miller, “Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage,” Proc. EEE Int’l Conf. Distributed Computing Systems (ICDCS ’06), 2006.
[2] A. Juels and J. Burton, S. Kaliski, “PORs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, Oct. 2007.
[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.
[4] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS ’07), pp.1-6, 2007.
[5] R.Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiple-Replica Provable Data Possession,” Proc. IEEE Int’l Conf. Distributed Computing Systems (ICDCS ’08), pp. 411-420, 2008.
[6] F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, “Efficient Remote Data Possession Checking in Critical Information Infrastructures,” IEEE Trans. Knowledge and Data Eng., Vol No. 20, pp. 1034-1038, Aug. 2008.
[7] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), Vol No.5350, pp. 90-107, Dec. 2008.
[8] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, “Dynamic Provable Data Possession,” Proc. ACM Conf. Computer and Comm. Security (CCS ’09), pp. 213-222, 2009.
[9] K.D. Bowers, A. Juels, and A. Oprea, “HAIL: A High-Availability and Integrity Layer for Cloud Storage,” Proc. ACM Conf. Computer and Comm. Security (CCS ’09), pp. 187-198, 2009.