International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Public Auditing and Data Dynamics in Cloud Data Storage

Snehal P. Sawant[1], Aaradhana. A. Deshmukh[2]

Department of Computer Science Engineering, Smt. Kashibai Navale College of Engineering Vadgaon, Pune, Maharashtra, India

Abstract: ***Now a days, cloud computing is emerged as a powerful tool for IT enterprise .Cloud computing is a next generation of 'utility computing', which provide services at a reasonable costs i.e. pay as you go. basically cloud computing comes into picture when we think about, what an IT enterprise in general needs i.e. a way to increase capacity or add capabilities, without investing capital in new infrastructure, or purchasing new software's. cloud computing provide services ranging from Software as a Service(SaaS), Platform as a Service(PaaS), Infrastructure as a Service(IaaS),Storage as a Service(SaaS) and many other services. In this paper we focus mainly on Storage as a service. In Storage as a service, a user puts his data on a cloud storage i.e. moving applications and data to the centralized data centers. But there may exist some security threats to that data and applications, as a cloud security is a major challenge in cloud computing. This paper studies the problem of data storage integrity in cloud computing. To simplify the task of verification of data integrity, we will take help of some Third Party Auditor (TPA), who will perform timely audit of data stored on a cloud, on behalf of client. The involvement of TPA eliminates the task of auditing that a client need to perform, to check whether his /her data is proper i.e. same as stored previously. In addition this paper focuses on data dynamics, which allow user to perform modifications to the data stored on a cloud, which may include block insertion, deletion etc. To achieve data dynamics we have applied the technique of merkle hash tree, instead of skip list (skip lists are used in previous works). In addition to auditing and data dynamics, the paper studies the efficient handling of multiple auditing tasks, by using the concept of bilinear aggregate signature, to enhance the auditing scheme where TPA can perform several auditing tasks simultaneously.***

Keywords: cloud computing, data storage integrity, public auditability and data dynamics, storage security

1. Introduction

Cloud computing is a recent trend in IT industry, which is growing rapidly. Basically cloud computing is an internet based service model, which provide on demand network access to a shared pool of configurable computing resources (e.g. networks, servers storage, applications, data etc) can be rapidly provided with a minimal management efforts, or service provider interaction. In short, cloud computing abstracts infrastructure complexities of servers, applications,data and heterogeneous platforms Cloud Computing allows user to access software's, applications without purchasing licensed copy of them; to use hardware and networks, platforms without establishing infrastructures; it provide metered usage of services i.e. pay as you go. Cloud enable user to access high quality services from data and software's residing on remote data center. Although could computing aim to provide promising, efficient service platform for internet, there are several security issues related to data stored on cloud. One of the most important concerns is data integrity verification at untrusted servers. For e.g. consider a situation where a service provider may hide certain data storage errors from client for their own benefit .i.e. to maintain their reputation. In some cases user may wish to perform some modifications, to the data stored on cloud, let the modification operation be block insertion, deletion and updation. At this stage, there should be some mechanism, which must ensure users that their data is kept appropriately intact all the time in the cloud. No matter how many times user perform changes to his data in cloud, the storage correctness should be maintained, even if users modify, delete or append their data files in the cloud. To solve the problem of data integrity verification, many schemes have been proposed under various models and systems. All the schemes of verification mainly fall into two categories private auditing and public auditing. The private auditing scheme have achieved efficient auditing as data is private and restrict access to particular limited users. However in public auditing not only the client/owner of data but also any one can challenge the integrity state of data. This paper introduces an entity i.e. Third Party Auditor (TPA), which relaxes the user from performing timely audit. As users may have busy hectic schedule, so he may not get time to perform timely audit, the TPA will perform audit ,on behalf of user and notify user if any one tries to steal their data or make changes to their data .another challenge in cloud security is supporting data dynamics i.e. when a user access remote data, he/she may wish to update their data through operations like block insertion, block modifications, deletions etc unfortunately till now this aspect is not been achieved in previous work, which mainly focuses on static data. It is very important to support data dynamics in order to achieve proper outsourcing of data. In short, this paper proposes:

1) Public auditing of data storage in cloud computing security and propose a scheme to enable data dynamism which was absent in previous schemes.
2) Second it proposes batch auditing, where TPA performs various auditing tasks simultaneously.
3) It also support dynamic operations on data to make sure that changes made by such operations should be reflected to the data stored on cloud properly to maintain data integrity of data stored on cloud.

2. Literature Review

Sr.no	*Author*	*Topic*	*Algorithm Applied*	*Advantages*	*Disadvantages*
1.	Q.wang [1]	Enabling public verifiability and data dynamics for storage in cloud computing.	Merkle hash tree and Bilinear map	Support verification with blockless and stateless verification features. Support dynamic operations on data.	This Scheme is uses the concept of Third Party Auditor (TPA), whose failure can affect the entire scheme.
2.	K.D.Bowers [3]	Proof of Retrievability: Theory and implementation.	Cryptographic Techniques With error correcting and spot checking codes.	Lower storage overhead. Tolerate higher error rates.	Though this scheme provides possession and retrievability, but it fails to achieve auditing and dynamic operations on data.
3.	C.Wang [4]	Ensuring data storage security in cloud.	Erasure correcting code.	This scheme supports the dynamic operations on data like data update, delete and append. Efficient against Byzantine failure, malicious attacks etc.	Though this scheme supports dynamic operations on data, it Not support insertion of data blocks in between the data.
4.	G.Ateniese [2]	Provable data possession at untrusted stores	RSA algo. & homomorphic verifiable Tags(HVT)	Allows a user whose data has been stored at untrusted server to verify that the server possesses the original data without retrieving it	Though this scheme supports auditing but it does not support dynamic operations on data as dynamic case may incur some design and security problems.
5.	Q.wang [5]	Enabling public auditability and data dynamics for storage in cloud computing.	Merkle hash tree and homomorphic authenticators, with erasure coded data.	User‘s verification task on data stored on cloud is hand over to a Third Party Auditor (TPA), which reduces user’s task and time. Also supports dynamic data operations such as data update, delete along with data insertion operation.	This scheme may suffer if TPA fails during any failure events.

3. Proposed System

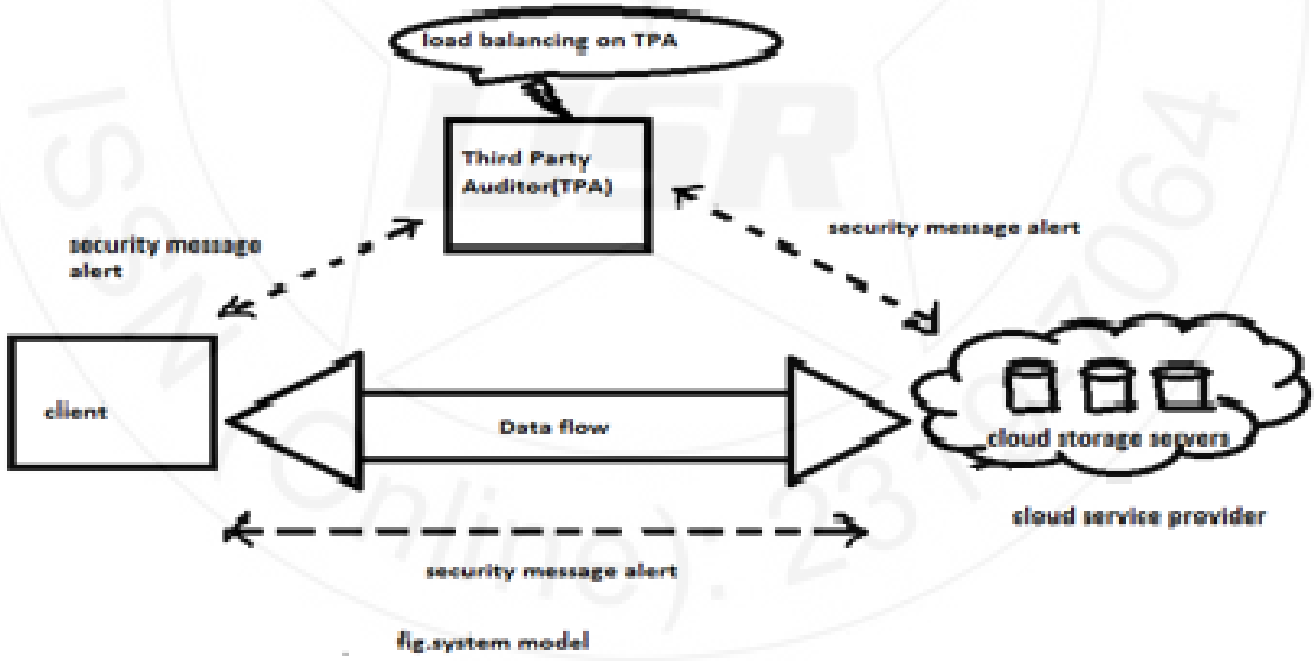

fig.system model

Above fig shows the system model.

The Proposed system consists of following entities:

1) **Client:**
Client is an entity, who possesses data files that he/she may wish to store on cloud and relies on cloud for further maintenance and operations. Client can be an individual or any organization, or a group of organizations having same policies or objectives.

2) **Cloud storage server**:
It is an entity, which possess significant amount of storage space as well as computational and network resources to manage client's data stored on cloud. Cloud storage server is managed by Cloud Service Provider (CSP).

3) **Third Party Auditor:(TPA)**
It is a trusted entity which is having skills, expertise and capabilities and TPA is allowed to assess the integrity of data stored on cloud by the client. TPA performs auditing of client's data stored on cloud On behalf of client. It periodically notifies the status of client's data to client this work also supports the dynamic operations on data such as block insertion, modification, deletion etc. To ensure that the modifications performed on the data are reflected properly to the data stored on cloud. I.e. to make sure data integrity is maintained.

4. Conclusion

As TPA is going to perform number of auditing tasks simultaneously, it is essential for this scheme to manage the load on TPA, so that it can perform auditing properly. Hence this work proposes to provide simultaneous auditing tasks by using Third Party Auditor (TPA) with dynamic data support.

References

[1] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Symp. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[2] 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.

[3] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Report 2008/175, Cryptology ePrint Archive, 2008

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.

[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li "Enabling10. Qian Wang, Cong Wang, Kui Ren , Wenjing Lou And Jin Li " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE transaction Paper on Parallel and Distributed Systems vol 22 No 5, pp. 847-859, May 2011.