Asian Journal of Convergence in Technology *Volume1, Issue 5*
Issn No.:2350-1146, I.F-2.71

ANALYSIS OF DATA SECURITY IN CLOUD USING THIRD PARTY AUDITOR: REVIEW

Ms.Tambe Vijayshree C.
Dept. of Computer Science Engineering
Bharat Ratna Indira Gandhi College of Engineering
Solapur,India
shree.tambe93@gmail.com

Prof. Jadhav Chandrakant M.
Dept. of Computer Science Engineering
Bharat Ratna Indira Gandhi College of Engineering
Solapur,India
chandaronly@gmail.com

Abstract— **Cloud is kind of centralized database where many organizations/clients store their data, retrieve data and possibly modify data. Data stored and retrieved in such a way may not be fully trustworthy so here concept of TPA(Third Party Auditor) is used. TPA makes task of client easy by verifying integrity of data stored on behalf of client. In cloud, there is support for data dynamics means clients can insert, delete or can update data so there should be security mechanism which ensure integrity for the same. Here TPA can not only see the data but he can access data or can modify also so there should be some security mechanism against this. Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. The introduction of effective TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing.**

Keywords— Cloud Computing, Third Party Auditor, Data Integrity,Encryption,Cloud Service Provider.

I. INTRODUCTION

Cloud data security is a major concern for the client while using the cloud services provided by the service provider. There can be some security issues and conflicts between the client and the service provider. To resolve those issues, a third party can be used as an auditor. In this paper, we have analysed various mechanisms to ensure reliable data storage using cloud services. It mainly focuses on the way of providing computing resources in form of service rather than a product and utilities are provided to users over internet. The cloud is a platform where data owner remotely store their data in cloud. The main goal of cloud computing concept is to secure and protect the data which come under the property of users. The security of cloud computing environment is exclusive research area which requires further development from both academic and research communities. In the corporate world there are a huge number of clients which is accessing the data and modifying the data. In the cloud, application and services move to centralized huge data center and services and management of this data may not be trustworthy, into cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. Third-party-auditor not only read but also may be change the data. Therefore a mechanism should be provided to solve the problem. We examine the problem contradiction between client and CSP, new potential security scheme used to solve problem. The purpose of this paper is to bring greater clarity landscape about cloud data security and their solution at user level using encryption algorithms which ensure the data owner and client that their data are intact. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. Since the security is not provided in cloud, many companies adopt their unique security structure. Introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle. One of the biggest concerns with cloud data storage is that of data integrity verification at un-trusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files. As data generation is far outpacing data storage it proves costly for small firms to frequently update their hardware whenever additional data is created. Also

maintaining the storages can be a difficult task. Storage outsourcing of data to cloud storage helps such firms by reducing the costs of storage, maintenance and personnel. It can also assure a reliable storage of important data by keeping multiple copies of the data thereby reducing the chance of losing data by hardware failures. Storing of user data in the cloud despite its advantages has many interesting security concerns which need to be extensively investigated for making it a reliable solution to the problem of avoiding local storage of data. In this paper we deal with the problem of implementing a protocol for obtaining a proof of data possession in the cloud sometimes referred to as Proof of retrievability (POR).This problem tries to obtain and verify a proof that the data that is stored by a user at a remote data storage in the cloud (called cloud storage archives or simply archives) is not modified by the archive and thereby the integrity of the data is assured. Such verification systems prevent the cloud storage archives from misrepresenting or modifying the data stored at it without the consent of the data owner by using frequent checks on the storage archives. Such checks must allow the data owner to efficiently, frequently, quickly and securely verify that the cloud archive is not cheating the owner. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and even serve for independent arbitration purposes.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. Various mechanisms are proposed on how to use the TPA so that it can relieve the burden of data owner for local data storage and maintenance; it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both individuals and enterprises with high service-level requirements. This kind of audit service not only helps save data owners,, computation resources but also provides a transparent yet cost- effective method for data owners to gain trust in the cloud. The presence of TPA eliminates the involvement of the client by auditing whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Though this method states how to save the computational resource and cost of storage of owner's data but how to trust on TPA that is not calculated. If TPA modifies data or deletes some data and if it becomes intrusive and pass information of data owner to unauthorized user than how owner know about this problem is not solved. Thus, new approaches are required to solve the above problem.

Before building the system the above consideration r taken into account for developing the proposed system. We have to analysis the Cloud Computing Outline Survey:

A. Cloud Computing

Cloud computing providing unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use.

- Benefits of Cloud Computing:
- Minimized Capital expenditure
- Location and Device independence
- Utilization and efficiency improvement
- Very high Scalability
- High Computing power

B. Security a major Concern:

- Security concerns arising because both customer data and program are residing in Provider Premises.
- Security is always a major concern in Open System Architectures.

C. Data centre Security?

- Professional Security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.
- When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked.
- All physical and electronic access to data centres by employees should be logged and audited routinely.
- Audit tools so that users can easily determine how their data is stored, protected, used, and verify policy enforcement.

D. Data Location:

- When user uses the cloud, user probably won't know exactly where your data is hosted, what country it will be stored in?
- Data should be stored and processed only in specific jurisdictions as define by user.

• Provider should also make a contractual commitment to obey local privacy requirements on behalf of their customers,

• Data-centered policies that are generated when a user provides personal or sensitive information that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy.

E. Backups of Data:

• Data store in database of provider should be redundantly store in multiple physical locations.

• Data that is generated during running of program on instances is all customer data and therefore provider should not perform backups.

• Control of Administrator on Databases.

F. Network Security:

• Denial of Service: where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service.

• QOS Violation: through congestion, delaying or dropping packets, or through resource hacking.

• Man in the Middle Attack: To overcome it always use SSL

• IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address.

G. How secure is encryption Scheme:

• Is it possible for all of my data to be fully encrypted?
• What algorithms are used?
• Who holds, maintains and issues the keys? Problem:
• Encryption accidents can make data totally unusable.
• Encryption can complicate availability Solution

• The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

III. EXISTING SYSTEM AND RELATED WORK

Cloud storage moves the user's data to large data centres, which are remotely located, on which user does not have any control. However, this unique feature of the cloud poses many new security challenges which need to be clearly understood and resolved. One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. One of the biggest concerns with cloud data storage is that of data integrity verification at un-trusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files.

Drawbacks of existing system

• TPA demands retrieval of user data, here privacy is not preserved

• TPA have to remember which key has been used

• These two schemes good for static data not for dynamic data.

IV. PROPOSED SYSTEM

The proposed problem is multi write and problem of TPA if Third-party-auditor not only uses data but also modify the data than how data owner or user will know about this problem. Here the user has two types' keys, one of which only the owner knows called private key and another one which is known to anyone called public key. We match both the data it must be same as the sent one on the sender cannot deny that they sent it (non repudiation). One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. To enable privacy-preserving public auditing for cloud data storage under the a for mentioned model, our protocol design should achieve the following security and performance guarantees. Public audit ability to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. Storage correctness to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact. This can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA). It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

V. SYSTEM ARCHITECTURAL FOCUS

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resor to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which

belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users.

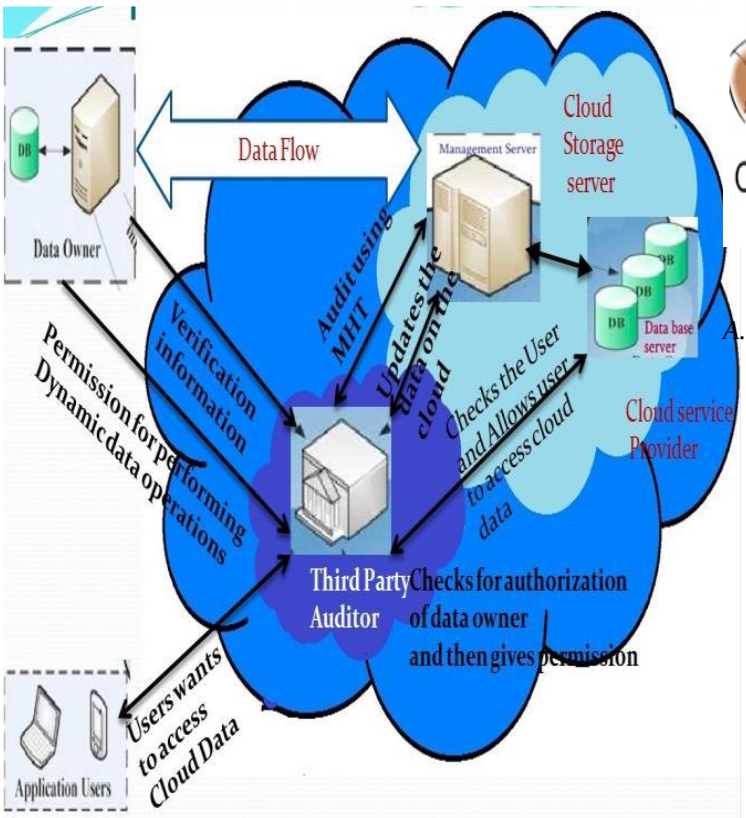

Fig 1: TPA which is used for auditing between public cloud and private cloud

A representative architecture for cloud data storage is illustrated in Fig. 2.Three different network entities can be identified as follows:

• Client: an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations;

• Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data.

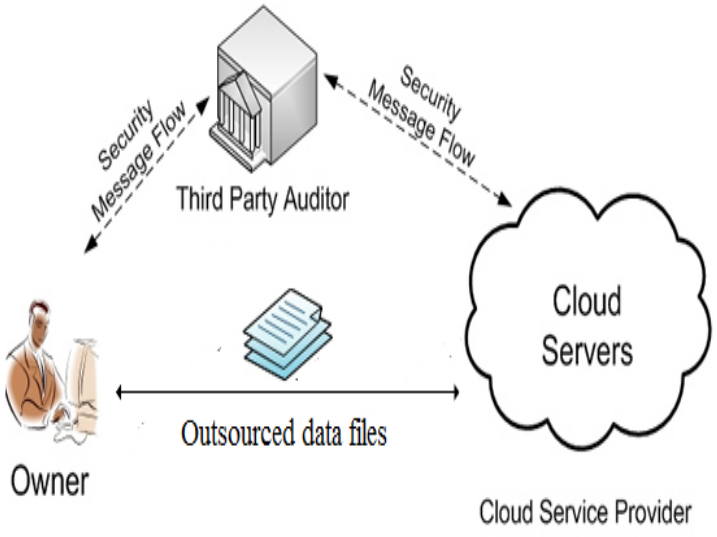

Fig.2: System Architecture

A. *Integrity Verification*

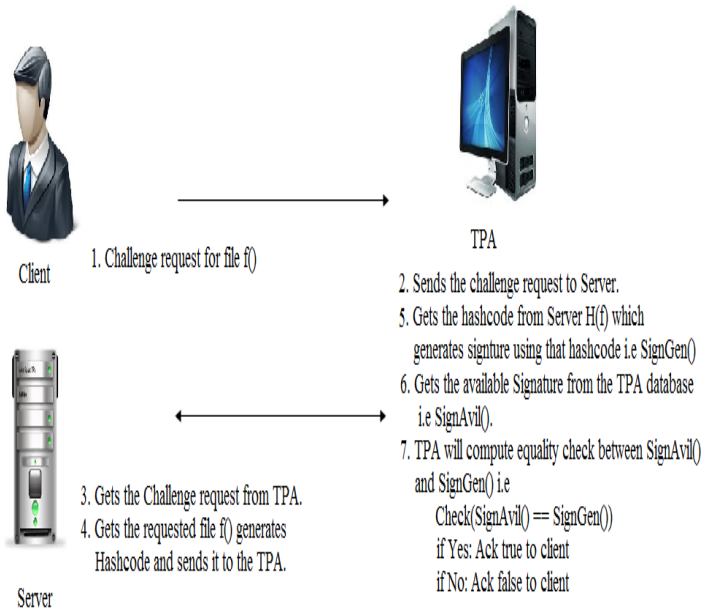

Fig.3: Protocol for Integrity Verification

The verifier before storing the file at the archive preprocesses the file and appends some Meta data to the file and stores at the archive. It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted. It does not prevent the archive from modifying the data.

In the following figure there are three important terms that is Client, Server and TPA (Third Party Auditor). Initially client will sends the integrity checking request to the TPA for file f(), TPA will forwards that request to the Server, Server will further fetches the respected file f() from the Server

database and generates the Hash code for that file i.e. h(f), and that will be send to the TPA with file name,TPA will generates the signature i.e. SigGen() from the hashcode sent by the Server, TPA will further fetches the old signature from the TPA database i.e. SigAvil(), inally TPA will does the equality check between the SigGen() and SigAvil() Ack will be sent to the Client depend upon the equality checking.In this way file integrity should be verified using this task successfully. This will be shown in the fig. 3.

B. Dynamic Data Operation with Integrity Assurance

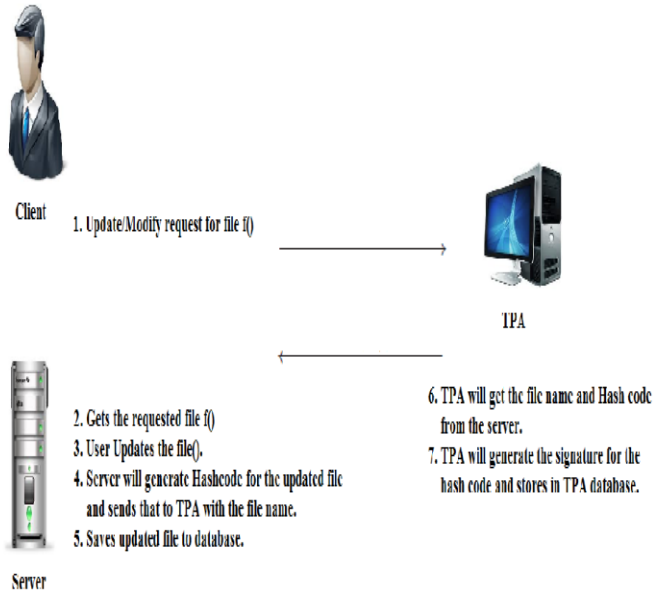

Fig.4: Protocol for provable data update

Now we show how our scheme can explicitly and efficiently handle fully dynamic data operations like Data Modification including data insertion (I) and data deletion (D) for cloud data storage. Note that in the following descriptions, we assume that the file F and the signature Sig() have already been generated and properly stored at server. The root metadata R has been signed by the client and stored at the cloud server, so that anyone who has the client's public key can challenge the correctness of data storage. Initially client sends modify request to Server for file f(), Server will fetches that respected file f() and allows client to modify or update his file, after modification by client Server will update the file and generates the hash code for the updated file and sends it to TPA with file name. TPA will generate Signature for the hash code which is sent by the Server and finally TPA updates the Signature in its database for future references. This will be shown in Fig.4. It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

VI. CONCLUSIONS

Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Various schemes are proposed by authors over the years to provide a trusted environment for cloud services. Encryption and Decryption algorithms are used to provide the security to user while using third party auditor. Here we have presented a data model for secure integrity verification scheme and with data update protocol that dynamic data modification by introducing effective third Party auditor. Here we provide a scheme which checks data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

Acknowledgment

First of all I would like to express my heartfelt thanks to Asst. Prof. Jadhav C.M. for their highly appreciable encouragement and support. Their guidance has been the constant driving force behind my preparation to this Paper. I would also like to thank my lecturers who have been instrumental in inspiring and motivating me with all career guidelines.I am grateful to all the suggestions and hints they have provided with respect to project. Finally, I would thank all my friends who have helped me in collecting the related materials and who have been responsible for improving the quality of this paper by discussing and providing me with the extra information related to the paper. I'm glad to admit that the paper has been a great learning experience and I would certainly look forward to future opportunities like this.

References

[1] C. Wang, Q. S.M. Chow, Kui Ren and Qian Wang, "Ensuring data storage security in cloud computing," in December 2011.

[2] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," Online https://www.sun.com/offers/details/sun transparency.xml, November 2009.

[3] M. Arrington, "Gmail disaster: Reports of mass email deletions,"2006 Online at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-aildeletions/December.

[4] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and secure sensor data storage with dynamic integrity assurance," in Proc. Of IEEE INFOCOM'09, Rio de Janeiro, Brazil, Appril 2009, pp. 954–962.

[5] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors,"at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[6] M. Naor and G. N. Rothblum, "The complexity of online memory checking," in *Proc. of FOCS'05*, Pittsburgh, PA, USA, 2005, pp. 573–584.

[7] E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," in *Proc. of ESORICS'08*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.

[8] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[9] A. Oprea, M. K. Reiter, and K. Yang, "Space-efficient block storage integrity," in *Proc. of NDSS'05*, San Diego, CA, USA, 2005.

[10] T. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in *Proc. of ICDCS'06*, Lisboa, Portugal, 2006, pp. 12–12.

[11] Xiang Tan and Bo Ai "The Issue of Cloud Computing Security in High-Speed Railway" international confer. on electronic and mechanical engi. And information technology, 2011. Beijing p.r china

[12] Farzad Sabahi,"Cloud Computing Security Threats and Responses",IEEE confer. 2011, 978-1-61284-486-2/111

[13] Ravi Kant Sahu and Abhishek Mohta, L.K. Awasthi "Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services", conf. IJARCSSE, 2012, Volume 2, Issue 2,ISSN: 2277 128X.

[14] Govinda V, and Gurunathaprasad, H Sathshkumar,"Third Party Auditing For Security Data Storage in cloud through digital signature using RSA" IJASATR, 2012, issue 2,vol-4, Issn 2249-9954.