A Survey on Cloud Storage Auditing Protocols

Shabana Shaik
CSE dept. G.Pullareddy engineering college
G.Pullareddy engineering college
Kurnool, India
shabanashaik0203@gmail.com

G.Vijay Kumar
CSE dept. G.Pullareddy engineering college
G.Pullareddy engineering college
Kurnool. India
gvjykumar.cse@gprec.ac.in

***Abstract*—** As Today's world depends on dynamically updated data, the best way to store and update data is cloud storage service. The common issue for storing data in cloud storage is its security though every individual client holds his/her own secret key the key service has to be supportive and is effective to the customer in different situations, so key redesign of outsourcing is important. The key overhauls can be handled by some authorized inspector known as TPA (Third Party Auditor) to reduce key upgrade burden from customer. It is the responsible of TPA now, to save key upgrades and makes key updates transparent for client. In existing solutions, client has to update key by himself at periodic times which leads to problem for those who need to concentrate on their main role in the market or with the people who have limited resources. This paper encloses a survey on the key exposure problem in cloud storage is formulated where the main goal is that cloud storage settings and key updates are safely outsourced to some third party where TPA can only hold encrypted version of client secret key formalizing security model. Security proof can be analyzed and make sure that design is secure and efficient.

Keywords*- Outsourcing computation, cloud storage auditing*

*****

I. INTRODUCTION

Cloud computing refers to shared pool of resources especially virtualized computer resources [1]. In general cloud computing is a market where unlimited services are been provided to millions of users all over the world. Cloud computing is totally based on Internet.

Cloud computing is a popular paradigm for storing data and providing unlimited service access to the users where there is great benefit from cloud, there exists many problems also with it. One such problem is Security [1]. Cloud Security deals with major aspects like integrity and confidentiality. Outsourcing computation playing major role these days since it is used in various applications like linear and algebraic computations including scientific applications. The storage problems arise due to less security of data.

Cloud computing obtains some features that made it extremely popular. It supports multitenancy and elastic in nature, cloud services are independent and accessible via internet, and it adopts pay per use policy with respect to the service provided to the user [8]. Usually cloud services also have different kinds that include Infrastructure which provide computer hardware resources, networking and storage as a service. Platform is a type of service that provides runtime environment to the user with a good flexibility and Application as a service that provides software applications, websites and many more. Now a day's many companies such as Amazon Web Services (AWS), SalesForce.com, GoogleAppEngine and many more provide unlimited services [8].

The term Cloud has some types such as public and private clouds. Public cloud is an open cloud to everyone with some features where as private cloud is limited to only an organization based on access control. The other clouds such as hybrid cloud obtain both features of both public and private and community cloud is for the group of people who acts a single group.

Owners of data worry about many problems like data loss in infrastructure or trust issues with cloud management. Integrity of data play major role in cloud storage to assure owners/clients if their data is safely stored.

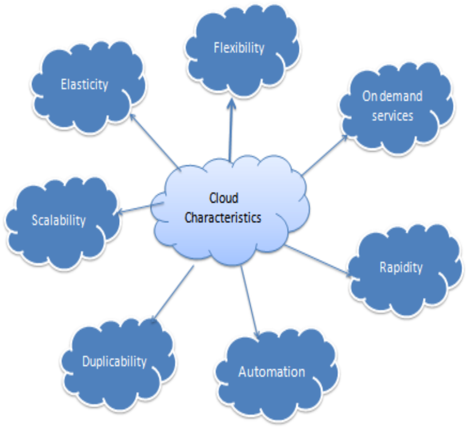


Figure. 1 Characteristics of cloud

II. BACKGROUND

is one of the major dynamic components that ensure that different machines on same platform are independent in nature [8]. It is also a difficult part to constantly maintain security for virtual machines and protect it from various errors. Under this, Para virtualization and Full virtualization are the two kinds in cloud paradigm. Para virtualization makes operating system work concurrently with each other whereas full virtualization is something where the entire hardware is replicated virtually. VMM Virtual Machine Monitor also a software element that provides virtual devices and processors such memory and storage. Vulnerability can be possible in any of cloud services so that a guest system get a access to read and write operation which is probably a kind of attack [8].

The common and compulsory element for cloud computing is Network and its Security. To deal with network attacks like DNS attack has to be clearly observed and avoided [10].

Since cloud storage adopts virtualization, various challenging problems arise time to time. The major such problem is security. Cloud user would definitely worry about their data if it can be lost in any infrastructure or sometimes cloud server can show dishonesty.

Earlier in 2013, a research were made in which the major threats of cloud services are failure of hardware systems and data loss, some traditional cryptographic methods were introduced to solve those problems, but these did not work to solve data integrity since techniques were outdated.

Data loss can occur in two cases, one among them is improper maintenance of data or deleting them without a backup plan second one is insufficient authentication and access control to unauthorized parties [10]. Failure of hardware systems means the physical damage to server or computer on which the entire process has to be done.

When talking about security these days, some common threats arise in the form of malicious insiders, a person or employee in an organization who cheats and collects sensitive data, to solve this there can be a way to restrict for employees and allow only internal employee who can be trusted that too within the network the access can be legal. A cloud storage service also faces some challenges regarding few attacks like SQL injection attack and Man in the Middle attack [9]. The former attack is something when the original code is replaced with attacker's code and the latter one is an attack that tries to interrupt in middle of any transaction or conversation. Other than these attacks, Sniffer attack, Denial of service attack and cross site scripting attack also a kind of problematic to deal with [9].

Some technologies authentication and identity, data encryption, information integrity and privacy, secure information management and some standard techniques to avoid attacks.

Here are the most challenging issues of cloud computing mentioned below:

- Service level Agreement
- Management of Platform
- Reliability and Availability of cloud standards
- Virtual machines
- Data Integrity
- Data Encryption

Service level agreement: It is a contract between cloud customer and cloud provider which address legal actions for corruption and also includes time of their service and many other services that provider has to assure to the customer. This becomes helpful when any vendor minimizes or deletes customer data. SLA helps to defend ourselves from any problem. SLA also maintains data protection, outages, and price structure.

Management of platform: Basically cloud has elastic environment under which the major capabilities are

- Building
- Deployment
- Integration
- Management

It is important because it has to manage on demand access, application providers, operating system support and remote storage.

Reliability and availability of cloud standards: These two factors becomes a problem when come to software services so cloud applications started to run locally and to make it reliable cloud even provides services on customer's desktop. If a customer has to trust cloud provider these two are the major things to assure customer with the features. These can also make trouble when there are slow network connections.

Virtual machines: One on Many or Many on One is a policy followed in virtual machines to balance load on data centres. Though machines run independently they utilize many migration techniques.

Data Encryption: It is the only and best way to save our data from any third person if the data is in encrypted version. Encryption and Decryption can help the best way and attackers could not easily decrypt in cloud storage since it uses complex standard algorithms and very expensive structure.

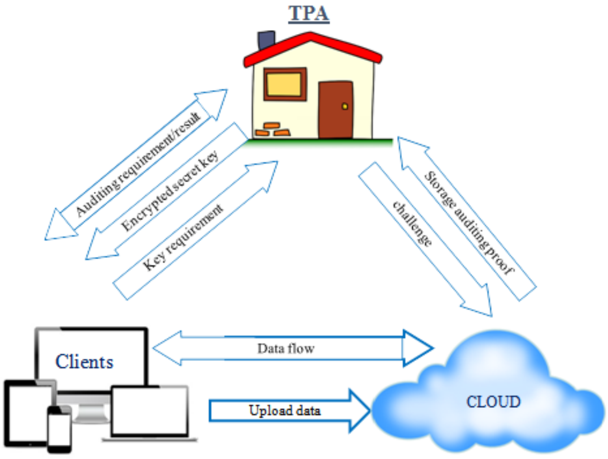
Data Integrity: It is necessary to achieve data integrity by maintaining through databases and constraints in database. Database transactions also important to held integrity in cloud computing. Data integrity is easy to maintain in standalone computers because of a single database whereas in distributed computer there are many issues to look after and method has to apply so that data is safely stored [10].

III. LITERATURE REVIEW

Auditing examines the management control of cloud systems. Audits are generally performed to verify system and applications, information processing facilities and system development.

Some protocols like dynamic auditing, Third party auditing, Batch auditing helps to execute cloud security. Under dynamic auditing, dynamic operations are performed and it make use of bilinearity property of bilinear pairing method so that it solves data privacy problem and batch auditing supports multiple owners and clouds also functions as a part in dynamic auditing[2]. These two auditing protocols combine and verify the proof of correctness and reduce auditors work load by moving data to the server. To provide privacy preserving auditing protocol cryptography method is anyway used. The proof between auditor and server to solve or to answer a challenge is a key role. This entire auditing system will improve its performance if the major techniques such as data fragment and homomorphic verifiable tags are applied in which data fragment technique reduces overload and by homomorphic verifiable tags, communication cost is reduced in between auditor and server. The process of this system starts from owner initialization, configuration auditing and sample auditing.

As per Jia yu and Kui ren [1], third party auditor plays the important role of updating secret keys and checks the integrity of client data. Here most advanced feature is TPA couldn't see the secret key, instead encrypted version of key is used. Outsourcing computation is the major topic to be discussed since it is used in many application domains. Initially hardware databases were used to perform such computations. The outsourcing algorithm proposed by Hohenberger and Lysyanskaya [2] determines precomputation methods and server aided computations. Outsourcing algorithms for attribute based signature, linear programming and homomorphic functions are introduced in this proposed system. Cloud storage auditing deals with provable data possession proposed by Ateniese et al [3] and proof of retrievability proposed by juels et al [4] to make sure that client data is safe from untrusted servers.



. Figure. 2 Process of cloud storage auditing

The above figure show TPA holds both client and cloud and perform key updates, hence TPA considered as powerful capability in performing computations. TPA need to update key according to time period and send encrypted key to client, client then decrypts it to get his real key, and can access files from cloud storage or update files.

Sometimes fair arbitration is necessary in between CSP and clients because in some cases both CSP and client can be dishonest in the operation. The best way to check honesty of either CSP or client is idea of signature exchange.

According to Hao Jin and Hong Jiang fair arbitration is necessary in the form of Third Party Arbitrator who is trusted by both parties.Third Party Arbitrator who resolves disputes adopts index switches to maintain mapping between block indices and tag indices, usually tag indices and block indices are used in tag computation or logical positions of data blocks. This index switches and dynamic auditing scheme is much explained in [5]

On the other hand Kang Yang and Xiaohua [6] proposed privacy preserving protocol so that data privacy protocol is solved. A method to prove encryption by using some technique named bilinearity property which helps to verify correctness of proof. The major aim to reduce communication cost between auditor and server. It performs security model so as to be secure from attacks like forgery, replace attack and replay attacks. Three phases of privacy preserving auditing protocol is discussed each with an efficient operation, apart from this batch auditing also involves for only multiple clouds with many owners.

Bi-Directional verification is an element which enforces both parties to verify with each other with the common platform entity, since TPA is unrealistic assumption for few cases, The Common platform plays crucial role of verifying, collects results and supervise the entire authorized parties. The major goal of bidirectional verification is low computation complexity and dynamic data operation support.

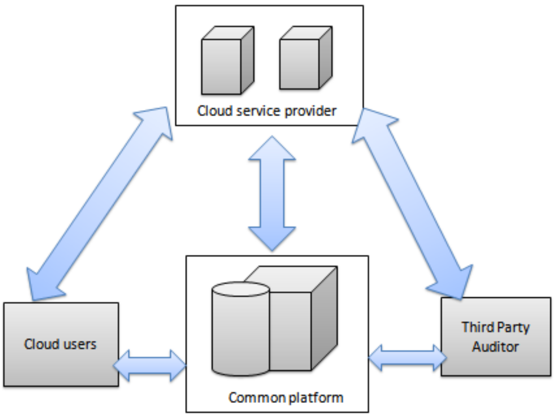


Figure. 3 Bi-Directional verification model

Kui Ren [1] also discussed in his paper about outages and security breaches also explained architecture how security messages flow between CSP and TPA's. The focus is on to ensure publicly auditable cloud services. Homomorphic security is used to avoid untrusted or semi trusted parties, public auditing minimizes auditing overhead and protect data with strong cryptography and data dynamics.

IV. OBSERVATIONS

The following table shows the outcomes and views of different authors around the world about auditing protocol and other different schemes that are necessary in cloud key security concept.

Reference No	Key Points	Advantages	Outcomes
[1]	Cloud storage, Outsourcing computation, Cloud auditing, Key update, Verifiability	Proof generation process, Proof verification process.	•Key updates are outsourced to TPA and transparent for the client and Client verifies the validity of encrypted secret keys
[2]	Dynamic auditing, Privacy preserving auditing, Batch auditing	Deals with various attacks and secure dynamic auditing operations.	•Combination of cryptography with bilinearity property of pairing protects data against auditor
[3]	Cloud computing, Cloud data security, Public auditing	Provides all basic knowledge of cloud related elements.	•Network Architecture for describing, developing and evaluating secure data storage problem

[4]	Integrity auditing, Public verifiability, Dynamic update, Arbitration, Fairness	Some theorems are proved in order to analyse the security along with fair arbitration.	Integrity auditing scheme with public verifiability, efficient data dynamics and Fair disputes arbitration between client and CSP
[5]	Provable data possession, Bi-Directional authentication	Error check, information gathering, Dynamic update are the operations.	•Remote data auditing system •Validation scheme to solve file errors •CSP verifies TPA'S authority

V. Conclusion

In this survey, determining how the auditing protocol gives formal security proof with encryption version so that data or security keys are outsourced safely to the cloud or client. Encryption algorithms are used such as AES and attribute based algorithm. In addition to this, client can be able to verify the validity of security keys when taking from TPA. The cloud storage auditing enables all this process transparent to client and reduce burden for client.

References

[1] Yu, Jia, Kui Ren, and Cong Wang. "Enabling cloud storage auditing with verifiable outsourcing of key updates." IEEE Transactions on Information Forensics and Security 11.6 (2016): 1362-1375J.

[2] Hohenberger, Susan, and Anna Lysyanskaya. "How to securely outsource cryptographic computations." Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2005.

[3] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." Infocom, 2010 proceedings ieee. Ieee, 2010.

[4] Juels, Ari, and Burton S. Kaliski Jr. "PORs: Proofs of retrievability for large files." Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.

[5] Jin, Hao, Hong Jiang, and Ke Zhou. "Dynamic and Public Auditing with Fair Arbitration for Cloud Data." IEEE Transactions on Cloud Computing(2016).

[6] Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." IEEE transactions on parallel and distributed systems 24.9 (2013): 1717-1726.

[7] Li, Yannan, et al. "Privacy preserving cloud data auditing with efficient key update." Future Generation Computer Systems 78 (2018): 789-798.

[8] Angadi, Abhinay B., Akshata B. Angadi, and Karuna C. Gull. "Security Issues with Possible Solutions in Cloud Computing-A Survey." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)2.2 (2013): pp-652.

[9] Srinivasamurthy, Shilpashree, and David Q. Liu. "Survey on cloud computing security." Proc. Conf. on Cloud Computing, CloudCom. Vol. 10. 2010.

[10] Gupta, Garima, P. R. Laxmi, and Shubhanjali Sharma. "A survey on cloud security issues and techniques." International Journal on Computational Sciences & Applications (IJCSA) 4 (2014): 125-132.