International Journal of Computer Applications (0975 – 8887)
Volume 162 – No 7, March 2017

Public Audit for Cloud Computing Environment: A Review

Tejashri A. Patil
Department of Computer Engineering,
SSBT's College Of Engineering & Technology,
North Maharashtra University,
Jalgaon, Maharashtra, India

Ashish T. Bhole
Department of Computer Engineering,
SSBT's College Of Engineering & Technology,
North Maharashtra University,
Jalgaon, Maharashtra, India

ABSTRACT
The cloud computing in its various form allow users to store information at remote location and reduce load at local system. Even though it is an advantage still drawback exists such as remote storage. The major security issues in cloud computing such as lack of data control, lack of trust and multi-tenancy are reviewed. The cloud computing and its service and deployment models are discussed by ways which the present security issues in cloud computing are prevented. Ensuring cloud data integrity and privacy seems to be the major issue. To overcome unauthorized access of data by cloud service providers and data users, verification is performed through trusted third party auditor. The cloud auditing needs to be performed and data security also needs to be ensured without the knowledge of the actual data stores at cloud. Researcher shows keen interest to provide a cloud framework, which preserves the privacy and ensures the integrity of cloud data. The paper reviews privacy preserving public audit schemes in cloud computing environment.

Keywords
Cloud environment, cloud computing, audit, trust, security

1. INTRODUCTION
Number of technologies are coming in the cloud computing, which provides Internet-based service and use of computer technology. storing data into the cloud storage offers great help to users since they do not have to care about the problems of hardware problems. As a result, users are at the interest of their cloud service providers for the availability and integrity of their data. On the one hand, although the cloud services are much more powerful and reliable than personal computing devices and broad range of both internal and external threats for data integrity still exist [1]. Everything is hosted in the cloud a nebulous assemblage of computers and servers accessed via the Internet. Cloud computing offers user to access all applications and documents from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate. Cloud computing is providing developers and organizations with the ability to focus on what matters most and avoids un-differentiated work like procurement, maintenance, and capacity plans. Cloud service providers have joined to build cloud environments and provide services to the user. Figure 1 shows tree structure of security issues regarding cloud data.

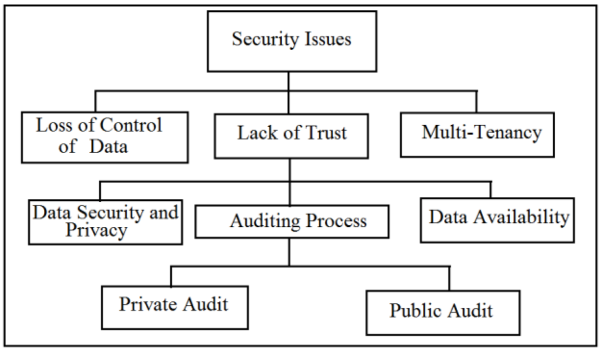

Figure 1 Security Issues of Cloud Computing

2. RELATED WORK
Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence it requires some secure and efficient methods which can ensure the integrity and privacy of data stored in the cloud.

2.1 Security Issues of Cloud Computing
The data processed in different clouds such as private and public clouds are subject to different security exposures. Therefore it is important to understand the various challenges associated with cloud computing [3]. These issues can be studied in terms of the following aspects:

- Loss of control of data
- Lack of trust
- Multi-tenancy

The users can lose the control over data in cloud computing because of the third-party models of the cloud. The data, applications, and resources are located with the provider; the user identity management is handled by the cloud; and the user-access control rules, security policies, and enforcement are managed by the cloud provider [8]. The consumer has to rely on the cloud provider for data security and privacy, and availability, and monitoring and repairing of services or resources. The cloud computing process is associated with certain risks due to loss of control in passing sensitive data to other organizations. In cloud computing, multi-tenancy refers to sharing of resources and services to run software instances that serve multiple consumers [15]. The main reason for cloud providers to have multi-tenancy is to reduce the costs by sharing and reusing resources among tenants. Here, the physical resources and services, as well as administrative functionality and support, can also be shared.

2.2 Cloud Auditing

Mostly Cloud environment is used to store large amount of data and permit the users to access the data from anywhere and at anytime. In the recent trend of storage technologies, instead of storing the data in hard drives like pen drives, compact discs, the data owners store their data in cloud for future references and access [2]. In case of data loss, the backup can be restored from cloud. Separate backup servers are also maintained by the cloud by considering any physical disasters in future[6] Since the data is stored remotely, the user needs to check the data periodically, whether it has been altered or not. The auditing process can be done by two ways:

- Private audit: The integrity of the data is verified by Data Owner.
- Public audit : The integrity of the data is verified by the TTPA

The user does not have the time, feasibility or resources to perform the storage correctness verification, he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable[4]. To securely introduce an eff ective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing [5]. That is why, using TPA services is a cost eff ective way for users to gain the trust in the cloud. The TPA has professional authenticate knowledge and audit skills.

2.3 Comparison of Auditing Techniques

Yua et al in [9] the active adversary attacks for two identity privacy-preserving auditing mechanisms namely Oruta and Knox, and a distributed storage integrity auditing mechanism. The author shows that these schemes are insecure when active adversaries are involved in the cloud storage and also can alter the data in the cloud, without knowing to the auditor in the cloud [7]. Technique of auditing more secure but Adversaries can Alters the data without knowing to auditor

In the Yang et Al in [10] proposed scheme, each and every group contains the group members and the group manager, maintained by the area manager. Many unauthorized users may modify the data stored in cloud without any identity. In order to overcome this issue, proposed an efficient public auditing solution that preserves the identity privacy and the identity traceability for group members simultaneously. Blind Signature technique of auditing is more secure but having more computation cost.

Digital signature auditing technique having less computation cost but it requires unbiased auditing service. Scheme proposed by Navajothi et al in[13] which focuses on efficient and secure cloud storage system and dynamic privacy-preserving audit service (TTPA) for verifying the integrity of outsourced storage. It achieves both public audit-ability and dynamic data operations.

To overcome the issue of dynamic management of outsourced data, data confidentiality and integrity, Kim et al in [11] proposed a public auditing protocol for educational multimedia data stored in the cloud using random values and a homomorphic hash function [14]. Even though cloud storage services provide a secure and reliable access to the outsourced educational multimedia data for users, it brings challenging security issues in terms of data confidentiality and integrity, and the some of the schemes also suffer from dynamic management of outsourced data.

Cloud storage provides the data storage in secured and effective way; the data gets affected due to the unauthorized access or some hardware/software failures. Yuchuan et al in [12] designed an auditing framework for cloud storage and proposed an algebraic signature based remote data possession checking protocol, which allows a third-party to auditing the integrity of the outsourced data on behalf of the users and supports unlimited number of verifications.

Table 1: Comparison of Audit Techniques for Cloud Computing

Author Name	Auditing Technique	Advantages	Disadvantages
Yua et al [9]	Qrta and knox	More Secure	Adversaries alters the data without knowing to author
Yang et al [10]	Blind Signature	More Secure	Heavy computation cost
Navjajothi et al [13]	Homo-morphic Hash function	Secure Supports full dynamic data	Additional computation cost
Kim et al [11]	Digital Signature	Less consumption cost	Requires unbiased auditing services
Yuchuan et al [12]	Algebric Signature	Efficient	More computation cost

The Table 1 shows comparison of auditing techniques. Trusted authority provides a unique global identification parameter to entities in the system. Data owner send request to third party auditors to perform auditing of data. Third party auditor launches the public auditing task by sending a challenge message to the Cloud Service Provider. The Cloud Service Provider will generate a response and send it to the TPA.

3. PROPOSED WORK

The approach used in proposed system is secure data in cloud storage. Cloud computing platforms provide easy access to a company high performance computing and storage infrastructure through web services.

3.1 Problem Statement

Most data storage centre helps the users to remotely store and access the data. People have failed to notice however, dynamic auditing cannot handle over encrypted data in cloud. By rethinking the approach to dynamic auditing process. Proposed system can fix the security challenges in auditing of encrypted data storage. To provide better solution, proposed public auditing protocols which support encrypted data and data dynamics. Proposed auditing protocol that is secured cloud storage auditing protocol efficiently handles encrypted data and performing auditing on encrypted data stored in cloud data.

3.2 Objectives

A secure and efficient privacy preserving public auditing scheme is to be proposed to achieve following objectives. It achieves privacy preserving and public auditing for cloud by using a TPA (Third Party Auditor), which does the auditing without retrieving the data copy, hence privacy is preserved.

1) Storage correctness
2) Privacy preservation
3) Searching over encrypted data
4) Auditing of cloud data

3.3 System Model

The main goal of proposed system is to secure and protect the data which come under the property of users. Figure 2 shows architecture of proposed system.

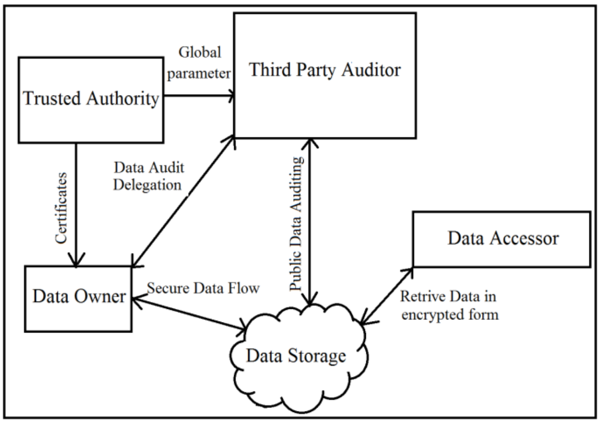

Figure 2 Proposed System Model

Data Accessor: An individual consumer or organization has a lot of data les and needs to store in the cloud. It depends on the cloud to manage data and computation, so it can reduce storage cost.

Data Storage: A cloud service provider has huge storage space and computation resource to provide the clients data.

Third Party Auditor: A trusted organization has expertise and capabilities that the clients do not have. It is responsible for assessing the client's data on cloud storage service.

Trusted Authority: Trusted authority provides certificates to data owner for identification purpose. Also provides global parameters to third party auditors.

Data Owner: Data owner upload data on cloud. Send request for checking integrity of data.

3.4 Proposed Algorithm

The data owner stores the data in the cloud initially. Instead of storing the entire data, the owner divides the data into multiple blocks and sends to the remote cloud storage [6]. If the data owner wants to check the integrity of content stored in cloud, initially a request message is made by the data owner to the TPA. The TPA receives the request message from data owner and sends a challenge message to the CSP, in order to verify the data. Once the CSP receives the challenge message from the TPA, it will send a response to TPA. Here the verification process is done by the TPA without having the knowledge of the original data. The TPA checks the data; it will provide the result to the data owner. The general framework given as follow:

- CertGen: The TA generates certificates and assign to data owners
- AssignPar: The TA assigns global parameters to TPAs.
- Setup: The data owner stores the data in cloud by dividing it into multiple numbers of blocks.
- KeyGen: The data owner generates a key using the large prime numbers. Using the large prime number, the public and the secret keys are generated by the data owner.
- SigGen: The data owner after generating the keys, will provides its own identity that it is by the true data owner, who stored it in cloud.
- Challenge: Once the keys are signed by the data owner, TPA wants to verify the data. So data owner sends a request to TPA regarding this. The TPA in turn will send a challenge message to the CSP.
- ProofGen: Once the CSP receives the challenge message from TPA, the CSP generates the proof and responds to TPA.
- ProofVerify: On receiving the proof the TPA verify the proof and finally it provides result to the data owner.

The proposed algorithm not only provides secure audit of cloud data but also prevents access to unauthorised users.

Algorithm stores data in cloud storage is as:

1) Start
2) Trusted authority generates global parameters for TPA and provides certificates to data owners.
3) Data owner select file an split it into number of blocks
4) Encrypt the blocks of file
5) Generate hash value for each block of file
6) Generate signature
7) Store encrypted file at cloud storage
8) End

Algorithm to perform audit operation is as:

1) Start
2) If data owner requires to perform audit
3) Send the signature to TPA
4) TPA requests for data to CSP
5) The TPA send challenge message to CSP
6) TPA verifies data integrity
7) CSP generates proof and responds to TPA
8) TPA sends verified proof to data owner
9) End

Algorithm to search over encrypted data is as:

1) Start
2) Data Accessor sends relevant query in encrypted form
3) Encrypted query evaluated at CSP
4) Results are generated in encrypted form

5) Results in encrypted form are send to data accessor
6) Data Accessor decrypts results
7) End

Execution flow of secure system model is shown in algorithm. Steps of algorithm are essential to prevent from unauthenticated users and impartial auditing by data owners into the cloud. Behalf of the two categories either public or private auditing, the public auditing is chosen by most of the researchers to provide a secured transaction and a secured integrity checking.

3.5 Basic Auditing Protocol

The basic auditing protocol by using all the semantics of a cloud storage auditing protocol. Figure 3 shows Framework of basic auditing protocol. TPA=(KeyGen,Outsource,Audit,Prove,Verify)

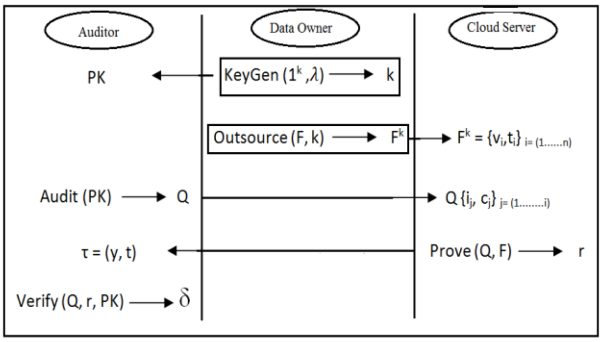

Figure 3 Framework of Basic Auditing Protocol

KeyGen(1k, λ) → K: The Data owner generates two random (safe) primes p, q of length k/2 each and then sets N = pq. In addition to k, assume an additional security parameter λ to generate the file identifier e, a prime number of (exactly) λ + 1 bits, greater than 2λ. Then the data owner determines the block length n and the total number of blocks m. The client also chooses g,g1,...,gn,h1,...,hm at random (in Z∗ N). The public key is PK = (N,e,g,g1,...,gn,h1,...,hm) and the secret key is SK = (p,q). Denote the key by K = (SK,PK).

Outsource(F; K) → F∗: On input the data F to be outsourced, the client divides F into a collection of vectors {vi = [vi1,...,vin]}i=1,2,...,m . For each vi, compute its signature as follows. First, generate a random integer si ∈ Ze uniformly. Use the Chinese remainder theorem to calculate xi ∈ZN by solving as given in equation 1.

$$x_i^e = g^{s_i} \cdot \left(\prod_{j=1}^{n} g_j^{v_j}\right) \cdot h_i \bmod N. \qquad (1)$$

Then the signature for vi is ti = (si,xi). The client then outsources the processed data F∗ = {vi,ti}i=1,2,...,m to the cloud server.

Audit(PK) → Q: Based on the public key PK provided by the client, the auditor runs this algorithm to generate a collection of indices and coefficients {ij,cj}j=1,2,...,l

where 1 ≤ ij ≤ m, cj ∈ N and l is the number of blocks the auditor queries. The auditor sends the query

Q = {ij,cj}j=1,2,...,l to the cloud server.

Prove(Q, F∗) → Γ: On receiving an audit query

Q = {ij,cj}j=1,2,...,l, where l is the length of the audit query. The cloud server first finds the signature (sij,xij) for each queried data block. Similar to linear network coding operations, the server then computes x using equation 2.

$$x = \frac{\prod_{j=1}^{l} x_{i_j}^{c_j}}{g^{s'} \prod_{j=1}^{n} g_j^{w'_j} \prod_{j=1}^{m} h_j^{w'_{n+j}}}. \qquad (2)$$

The server extracts the first n entries of w as a vector y ∈ Zn e and the signature of y is t = (s, x). The server sends back Γ = (y,t) as a proof of the corresponding query.

Verify(Q, Γ; PK) → δ: On input of an audit query

Q = {ij,cj}j=1,2,...,l, The server's proof Γ = (y,t), the auditor constructs a vector w such that the first n entries of w are the same as y, the (n + ij)-entry is cj, and all other entries are 0. If they are equal, the integrity of the file is verified as correct and output δ = 1; else, the integrity of the file is verified as incorrect and output δ = 0.

4. CONCLUSION

In cloud storage service, the data integrity of remote verification is a critical issue. The concept of public audit solves data integrity problem by remote verification of shared data. Study different representative approaches and analyze these approaches. Comparison table clearly understand the advantages and disadvantages of each approach. Public auditing schemes need to ensure data privacy, provide easy accessibility and prevent from unauthenticated user. A secure and efficient privacy preserving public auditing scheme is been proposed. It achieves privacy preserving and public auditing for cloud by using a Third Party Auditor, which does the auditing without retrieving the data copy, hence privacy is preserved. The data integrity is verified by TPA on request of the client by verifying both the signatures. The public auditing is chosen by most of the researchers to provide a secured transaction and a secured integrity checking.

In future, the data security and privacy can be enhanced with modern auditing techniques for cloud computing and secure cloud framework can be formed from un-authorized users.

5. REFERENCES

[1] Sookhak, Mehdi, Abdullah Gani, Muhammad Khurram Khan, and Rajkumar Buyya. *"Dynamic remote data auditing for securing big data storage in cloud computing."* Information Sciences 380 (2017): 101-116

[2] Kim, Daeyeong, Hyunsoo Kwon, Changhee Hahn, and Junbeom Hur. *"Privacy-preserving public auditing for educational multimedia data in cloud computing."* Multimedia Tools and Applications 75, no. 21 (2016): 13077-13091

[3] Ateniese, Giuseppe, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik. *"Scalable and efficient provable data possession."* In Proceedings of the 4th international conference on Security and privacy in communication netowrks, p. 9. ACM, 2008

[4] Shimbre, Nivedita, and Priya Deshpande. *"Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm."* In Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on, pp. 35-39. IEEE, 2015

[5] Cao, Ning, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. "*Privacy-preserving multi-keyword ranked search*

over encrypted cloud data." IEEE Transactions on parallel and distributed systems 25, no. 1 (2014): 222-233

[6] Lordemann, David, Daniel Robinson, and Paul Scheibe. *"Method and system for establishing an audit trail to protect objects distributed over a network."* U.S. Patent Application 09/952,696, filed September 14, 2001

[7] 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, no. 9 (2013): 1717-1726

[8] Li, Ling, Lin Xu, Jing Li, and Changchun Zhang. *"Study on the third-party audit in cloud storage service."* In Cloud and Service Computing (CSC), 2011 International Conference on, pp. 220-227. IEEE, 2011

[9] Yu, Yong, Lei Niu, Guomin Yang, Yi Mu, and Willy Susilo. *"On the security of auditing mechanisms for secure cloud storage."* Future Generation Computer Systems 30 (2014): 127-132

[10] Yang, Guangyang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu, and Rong Hao. *"Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability."* Journal of Systems and Software 113 (2016): 130-139

[11] Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. *"Privacy-preserving public auditing for data storage security in cloud computing."* In Infocom, 2010 proceedings IEEE, pp. 1-9. IEEE, 2010

[12] Yuchuan, Luo, Fu Shaojing, Xu Ming, and Wang Dongsheng. "Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage." China Communications 11, no. 11 (2014): 114-124

[13] Navajothi, R., and S. Jean Adrien Fenelon. *"An efficient, dynamic, privacy preserving public auditing method on untrusted cloud storage."* In Information Communication and Embedded Systems (ICICES), 2014 International Conference on, pp. 1-6. IEEE, 2014

[14] Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing, (2012) ―Towared secure and Dependable storage service in cloud computing, IEEE

[15] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, ―Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility, Fut. Gener. Comput. Syst., pp. 599–616, 2009